TEKNILLINEN KORKEAKOULU

Sähkö- ja tietoliikennetekniikan osasto

Sampsamatti Artturi Tanner

Leimakytkentäisten virtuaaliverkkojen yhteenliittämistapojen vertailu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 13.6.2007.

Työn valvoja: Professori Raimo Kantola

Työn ohjaaja: DI Johan Laxén

TEKNILLINEN KORKEAKOULU DIPLOMITYÖN TIIVISTELMÄ

Tekijä:	Sampsamatti Artturi Tanner
Työn nimi:	Leimakytkentäisten virtuaaliverkkojen yhteenliittämistapojen vertailu
Päivämäärä:	13.6.2007
Sivumäärä:	117
Osasto:	Sähkö- ja tietoliikennetekniikan osasto
Professuuri:	S-38 Tietoverkkotekniikka
Työn valvoja:	Professori Raimo Kantola
Työn ohjaaja:	DI Johan Laxén

Operaattorit tarjoavat leimakytkentää hyödyntäviä virtuaaliverkkopalveluita asiakkailleen. Lisäksi operaattorit hyödyntävät niitä omien palveluidensa tuottamisessa. Sekä leimakytkentä että sitä hyödyntävät virtuaaliverkkopalvelut on määritelty toimiviksi yhden autonomisen alueen sisällä. Tässä työssä vertaillaan neljää erilaista tapaa liittää virtuaaliverkot toimimaan yli AS-rajojen. Vertailu tehdään tietoturvallisuuden näkökulmasta.

Työssä paneudutaan kolmeen eri virtuaaliverkkopalveluun ja siihen, miten näiden toteutustekniikat vaikuttavat yhteenliittämiseen. Vertailu on pyritty tekemään niin, että se on sovellettavissa kaikille palveluille. Kaikilta osilta näin ei ole, sillä palveluiden toteutustavat poikkeavat liikaa toisistaan.

Vertailu paljasti, että yhteenliittämistavoilla on erilaisia vahvuuksia tietoturvan suhteen. Yhteenliittämistapaa valitessa operaattorin tulee määritellä, mitä tietoturvauhkia painottaa. Osa tietoturvauhista johtuu laitevalmistajien toteutuksien heikkouksista, mutta osa on standardeille ominaisia. Tietoturvariskit tiedostaen, ja ottamalla huomioon yhteenliittämisen aiheuttamat lisäriskit tietoturvalle, operaattorin on mahdollista tarjota tietoturvallisia leimakytkentäisiä virtuaaliverkkopalveluita, jotka kattavat useamman autonomisen alueen.

AVAINSANAT:	Leimakytkentä, MPLS, virtuaaliverkko, VPN, tietoturva, vertailu

HELSINKI UNIVERSITY OF TECHNOLOGY ABSTRACT OF THE MASTER'S THESIS

Author:	Sampsamatti Artturi Tanner
Name of the Thesis:	Comparing interconnecting methods for Multiprotocol Label Switched Virtual Private Networks
Date:	13.6.2007
Number of pages:	117
Department:	Department of Electrical and Communications Engineering
Professorship:	S-38 Networking Technology
Supervisor:	Professor Raimo Kantola
Instructor:	M.Sc. (Tech.) Johan Laxén

Telecommunication operators offer Multiprotocol Label Switched Virtual Private Networks to their customers. Also, MPLS VPN technologies can be used for operators' internal purposes, to enable them to offer wider range of services in single infrastructure. Both MPLS and MPLS based VPNs are defined to be used inside single autonomous system, AS. The aim of this thesis is to compare four different interconnection methods for MPLS VPNs in different AS's. The focus is on security.

Three different MPLS VPN services are looked into closely. Each service's technology's effect on interconnection is of interest. The comparison tries to incorporate all three services. But, since the services differ from each other, not all criteria concern all services.

The comparison revealed that the interconnection methods have different strengths concerning security. When choosing the interconnection method, an operator needs to define what areas of security it finds relevant. A portion of security issues are implementation specific, but some come directly from the standards. When operator is aware of the security issues related to chosen interconnection method, it is safe to offer MPLS VPNs that cover multiple autonomous systems.

KEYWORDS:	Multiprotocol Label Switching, MPLS, Virtual Private Networks, VPN, Security, comparison

ALKULAUSE

”As there is still no standard for carrier-carrier MPLS it is not possible to have the same MPLS service (Layer2 or Layer3 VPN) covering more than one operator.” – Wikipedia [Wik07]

Tämän työn valvojana toiminutta professori Raimo Kantolaa kiitän hänen kommenteistaan, neuvoistaan sekä kiinnostuksestaan työtäni kohtaan. Hänen ehdottamansa suomenkieliset termit paransivat työn luettavuutta.

Työn ohjaajana toimi DI Johan Laxén TeliaSoneralta. Häntä haluan kiittää pitkäjännitteisestä yhteistyöstä diplomityöni eri vaiheissa. Haluan myös kiittää muita teliasoneralaisia saamastani tuesta tehdessäni diplomityötäni työn ohessa. Erityiskiitokset haluan antaa Harry Lindbergille, joka on tehnyt ison työn auttamalla monissa työn vaiheissa kommentoinnillaan ja keskustelukumppanina.

Lopuksi haluan kiittää Miannaa, joka sekä toimi työn kielen tarkastajana että antoi minulle kirjoitusrauhan ottamalla päävastuun perheemme pyörittämisestä useamman kuukauden ajan, ja Eljasta, jonka ”Vieläkö sä kirjoitat?” –kysymykset antoivat kummasti potkua työn loppuunsaattamiseen.

Helsingissä, kesäkuun 7. päivänä 2007

Sampsamatti Tanner

SISÄLLYSLUETTELO

Lyhenne- ja Termistöluettelo

Lyhenne	Alkukielinen termi	Työssä käytetyt termit, *selitys*
AC	Access Circuit, Access Connection, Attachment VC	Asiakasyhteys, liitäntäpiiri, *kytkee asiakaslaitteen operaattorin laitteeseen*
AS	Autonomous System	AS, autonominen alue, *verkkokokonaisuus, jolla on yhtenäinen hallinto ja reitityspolitiikka*
ASBR	Autonomous System Border Router	ASBR, ASBR-reititin, rajareititin *autonomisen alueen rajalla oleva reititin, joka on yhteydessä myös toiseen AS:ään*
ASN	Autonomous System Number	ASN, AS-numero, *RIR:n operaattorille myöntämä yksilöllinen numeerinen tunniste*
ATM	Asynchronous Transfer Mode	ATM, *verkkotekniikka, jota käytetään lähinnä pysyvien pisteestä—pisteeseen –linkkien luontiin*
BGP	Border Gateway Protocol	BGP, BGP-protokolla, *autonomisten alueiden välinen reititysprotokolla*
BGP-MP	BGP Multiprotocol Extensions	BGP-MP, BGP:n moniprotokollalaajennus, *tapa, jolla BGP:ssä voidaan välittää tietoa muustakin kuin unicast-IPv4-reiteistä*
CE	Customer Edge (device)	CE, CE-laite, CE-reititin, *asiakasverkon laite, joka kytkeytyy PE-laitteeseen*
CsC	Carriers' Carrier	CsC, *L3-VPN-toteutus, jossa asiakasyhteydellä käytetään leimakytkentää*
eBGP	external BGP	eBGP, *käytetään BGP-yhteyksistä, kun halutaan korostaa niiden olevan autonomisten alueiden välisiä*
FEC	Forwarding Equivalence Class	FEC, kytkentäluokka, *joukko paketteja, joita kohdellaan leimakytketyssä verkossa yhdenmukaisesti*
FRR	Fast Reroute	FRR, *RSVP-TE:hen perustuva nopea vikapaikan ohikytkentä*
HDLC	High-level Data Link Control	HDLC, *OSI:n linkkikerroksen protokolla*

iBGP	internal BGP	iBGP, *käytetään BGP-yhteyksistä, kun halutaan korostaa niiden olevan autonomisten alueiden sisäisiä*
I-D	Internet Draft	I-D, Internet-drafti, *työn alla oleva IETF:n dokumentti*
IETF	Internet Engineering Task Force	IETF, *kansainvälinen organisaatio, joka pääsääntöisesti vastaa Internet-teknologioiden standardoinnista*
IGP	Interior Gateway Protocol	IGP, IGP-protokolla, *yleisnimitys autonomisen alueen sisäisille reititysprotokollille*
IP	Internet Protocol	IP, IP-protokolla
IPsec	Internet Protocol Security	IPsec, *joukko IETF:n määrittelemiä IP-protokollan laajennuksia, joilla pyritään lisäämään IP-viestinnän turvallisuutta*
ISO	International Standardization Organization	ISO, *Kansainvälinen standardointiliitto*
IS-IS	Intermediate System to Intermediate System (protocol)	IS-IS, IS-IS-protokolla, *eräs IGP-reititysprotokolla*
ITU	International Telecommunication Union	ITU, *YK:n alainen tietoliikennealan standardointi- ja kehitysjärjestö*
ITU-T	ITU - Telecommunication standardization sector	ITU-T, *ITU:n osaorganisaatio, joka antaa ja tekee tietoliikennealan suosituksia*
L2	Layer 2	L2, siirtoyhteyskerros, toinen kerros, *OSI-mallin mukainen siirtoyhteyskerros, esim. Ethernet*
L2TP	Layer 2 Tunneling Protocol	L2TP, *IETF:n määrittelemä tapa tunneloida PPP-yhteys minkä tahansa pakettiverkon yli*
L2vpn	Layer 2 Virtual Private Networks	L2vpn, L2vpn-työryhmä, *IETF:n työryhmä, joka standardoi virtuaaliverkkopalveluita, jotka tarjoavat asiakkaille L2-yhteyden operaattorin pakettiverkon yli*
L2-VPN	Layer 2 Virtual Private Network	L2-VPN, L2-virtuaaliverkko, v*irtuaaliverkko, joka tarjoaa siirtoyhteyskerroksen mukaisen yhteyden toimipisteiden välille*

L3	Layer 3	L3, verkkokerros, kolmas kerros, *OSI-mallin mukainen verkkokerros, tässä työssä lähinnä IP*
L3vpn	Layer 3 Virtual Private Networks	L3vpn, L3vpn-työryhmä, *IETF:n työryhmä, joka standardoi virtuaaliverkkopalveluita, jotka tarjoavat asiakkaiden käyttöön yksityisen IP-verkon operaattorin verkon yli*
L3-VPN	Layer 3 Virtual Private Network	L3-VPN, L3-virtuaaliverkko, v*irtuaaliverkko, joka tarjoaa verkkokerroksen – lähinnä IP:n – mukaisen yhteyden toimipisteiden välille*
LDP	Label Distribution Protocol	LDP, LDP-protokolla, *eräs leimojenlevitysprotokolla*
LER	Label Edge Router	LER, (Leimaverkon) reunareititin, *leimaverkon reunalla oleva LSR-reititin, joka välittää leimatonta liikennettä leimakytkettyyn verkkoon ja liikennettä leimaverkosta leimattomaan*
LSP	Label Switched Path	LSP, leimakytketty polku, leimapolku, *reitti, jota pitkin tietyn FEC:n omaavat paketit kulkevat leimakytketyssä verkossa*
LSR	Label Switching Router	LSR, Leimareititin, *reititin, joka käsittelee leimoja ja leimakytkettyä liikennettä*
MD5	Message-Digest algorithm 5	MD5, *algoritmi, jolla merkkijonolle voidaan laskea tiiviste. Tällä tiivisteellä varmistetaan, ettei merkkijono ole muuttunut siirron aikana*
MPLS	Multiprotocol Label Switching	MPLS, leimakytkentä, *IETF:n standardoima leimakytkentätekniikka*
OAM	Operation, Administration & Maintenance	OAM, *nimitys hallintatarkoituksiin käytetylle asialle*
OSI	Open Systems Interconnection (model)	OSI-malli, *ISO:n standardoima yhteyskäytäntökokonaisuuksia kuvaava malli*
OSPF	Open Shortest Path First	OSPF, OSPF-protokolla, *eräs IGP-reititysprotokolla*

PE	Provider Edge	PE, PE-reititin, palvelun reunareititin, *operaattorin reititin, johon VPN-asiakkaat kytkeytyvät*
PPP	Point-to-Point Protocol	PPP, *yksinkertainen protokolla, jolla voidaan kuljettaa datagrammeja pisteestä pisteeseen -yhteyden yli*
PW	Pseudo wire	PW, Virtuaalijohdin
RD	Route Distinguisher	Reittierotin, RD, *BGP-reitityksessä VPN-osoitteisiin lisätty tunniste, jonka avulla VPN-osoitteiden yksilöllisyys voidaan varmistaa*
R_d	Downstream Router	R_d, alavirran reititin, *paketin kulkusuuntaa tarkasteltaessa vastaanottava reititin*
RFC	Request For Comments	RFC, *IETF:n julkaistu dokumentti, jolla on pysyvä tunnusnumero*
RIPE	Réseaux Internet protocol Européens	RIPE, *eurooppalainen avoin järjestö, joka luo ja ylläpitää Internetin politiikkaa (esim. osoitejaon suhteen). RIPE NCC toimii RIPE:n ohjeistuksen mukaan.*
RIPE NCC	RIPE Network Coordination Centre	RIPE NCC, *Euroopan alueellinen Internet-rekisteri*
RIR	Regional Internet Registry	RIR, alueellinen Internet-rekisteri, *IP-osoitteita ja AS-numeroita hallinnoiva elin. Euroopassa RIPE NCC*
RR	Route Reflector	RR, BGP-reittiheijastin, reittiheijastin, *verkossa oleva toiminne, joka toimii BGP-signaloinnin välityspisteenä. Sijaitsee yleensä reitittimessä*
RSVP	Resource ReSerVation Protocol	RSVP, RSVP-protokolla
RSVP-TE	Extensions to RSVP for LSP Tunnels	RSVP-TE, *RSVP-protokollan käyttäminen leimojenlevitysprotokollana*
RT	Route Target	Kohdesuodin, RT, *VPN-reitteihin BGP:ssä liitettävä attribuutti, jota käytetään VPN-reitityksen apuna*
R_u	Upstream Router	R_u, ylävirran reititin, *paketin kulkusuuntaa tarkasteltaessa lähettävä reititin*

S-PE	PW Switching Provider Edge	S-PE, *moniosaisessa virtuaalijohtimessa virtuaalijohtimia kytkevä reititin, jossa ei ole asiakasliitäntöjä*
T-PE	PW Terminating Provider Edge	T-PE, *moniosaisessa virtuaalijohtimessa virtuaalijohtimia kytkevä reititin, johon asiakasyhteys on kytketty*
VC	Virtual Channel	VC, virtuaalikanava, *ATM-verkkoon luotu pisteestä-pisteeseen -yhteys*
VCI	Virtual Channel Identifier	VCI, *ATM-kanavan tunniste*
VLAN	Virtual LAN	VLAN, *tekniikka, jolla samaan fyysiseen Ethernet-lähiverkkoon luodaan loogisesti erillisiä lähiverkkoja*
VPI	Virtual Path Identifier	VPI, *ATM-polun tunniste*
VPN	Virtual Private Network	VPN, virtuaaliverkko, *yhteisessä käytössä olevia laitteistoja hyödyntävä, näennäisesti yksityisessä käytössä oleva, verkko*
VRF	VPN Routing and Forwarding table	VRF, VRF-taulu, *virtuaaliverkkokohtainen reititys- ja kytkentätaulu*
VRI	VPN forwarding instance	VRI, *virtuaaliverkkokohtainen reititys- ja kytkentätoiminne PE-reitittimessä*
WAN	Wide Area Network	WAN
YK	United Nations	Yhdistyneet Kansakunnat
-	Control Plane	Pakettiliikenteen hallintataso
-	Data Plane	Pakettiliikenteen välitystaso
-	Site	Toimipiste, *operaattorin verkkoon liittyvä kokonaisuus, usein lähiverkko*
-	VPN topology	VPN-topologia, *VPN-palvelun avulla muodostuva verkkotopologia*
-	Zone of trust	luottamusalue, *kokonaisuus, joka ajatellaan turvalliseksi tietyssä tarkastelussa*

KUVALUETTELO

luku 1:
Johdanto

Operaattorit ovat kehittämässä verkkojaan monipalveluverkkoideologian mukaisesti tavoitteenaan yksi runkoverkko, jonka varassa monet nykyisin eri verkoissa tuotetut palvelut voisivat toimia. Leimakytkentätekniikalla (MPLS) on monipalveluverkon toteuttamisessa keskeinen asema. Virtuaaliverkkopalveluiden (VPN:t) tarjoaminen asiakkaille on tärkeä leimakytkennän operaattorille tuoma mahdollisuus. MPLS-VPN:iä voidaan hyödyntää myös operaattorin sisäisessä toiminnassa.

Leimakytkennän avulla toteutetut virtuaaliverkot toimivat lähtökohtaisesti vain yhden hallinnollisen verkon eli autonomisen alueen (AS) sisällä. Operaattoreilla on tarvetta laajentaa virtuaaliverkkopalvelun kattavuutta yli AS-rajojen, koska yhdellä operaattorilla voi olla käytössä useampia erillisiä autonomisia alueita ja koska operaattoreilla saattaa olla tarvetta laajentaa virtuaaliverkkopalvelun kattavuutta toisten operaattoreiden alueille (yhteistyössä niiden kanssa). Tulevaisuuden liityntäverkot lienevät valtaosin leimakytkennän avulla toteutettuja metroethernet-verkkoja. Liityntäverkkojen yhteiskäyttö useamman operaattorin kesken voi myös hyödyntää leimakytkentäisten virtuaaliverkojen yhteenliittämistä. Jotta virtuaaliverkkopalvelut toimisivat useamman autonomisen alueen "yli" tietoturvallisesti ja tehokkaasti, on yhteenliittämistapaan syytä paneutua.

MPLS-VPN-palveluita voidaan laajentaa kattamaan useat autonomiset alueet usealla eri tavalla. Internet-tekniikoita standardoivan Internet Engineering Task Forcen (IETF) huomio on ensisijaisesti ollut eri virtuaaliverkkopalveluiden standardoinnissa toimiviksi yhden autonomisen alueen sisällä, joten se on vasta standardoimassa AS:ien välistä toimintaa. Sama on tilanne myös joitakin MPLS-VPN-suosituksia julkaisseella Yhdistyneiden Kansakuntien alaisella tietoliikennealan standardointi- ja kehitysjärjestöllä ITU-T:llä. Myöskään leimakytkentäaihepiirissä työskentelevä MFA Forum (entiseltä nimeltään MPLS Forum) ei ole julkaissut aiheesta suosituksia. Suurimmat reititinvalmistajat ovat julkaisseet aihepiiriin liittyen joitakin dokumentteja, mutta niissä ei ole verrattu eri toteutustapoja systemaattisella tavalla keskenään, eikä näissä, lähinnä konfigurointiohjeiksi luokiteltavissa dokumenteissa, muutenkaan pohdita ratkaisujen eri puolia kovin laajalti.

Tietoturvallisuus on erottamaton osa tietoliikenneoperaattorin toimintaa. Erityisesti tämä korostuu virtuaaliverkkopalveluissa, joita tarjotaan julkista verkkoa tietoturvallisempana vaihtoehtona toimipisteiden väliseen liikennöintiin. Tietoturvaa on käytetty mielestäni varsin ylimalkaisesti perustelemaan jonkin yhteenliittämistavan paremmuutta muihin verrattuna, kuitenkaan erittelemättä miten ja missä tilanteissa tämä paremmuus tulee ilmi.

Leimakytkentään perustuvien virtuaaliverkkopalveluiden yleistyessä, standardien vakiintuessa ja kilpailun kovetessa, kasvaa operaattorin tarve löytää hyvä, kaikki tarjotut virtuaaliverkkopalvelut kattava, ratkaisu liittää eri AS:t yhteen maantieteellisesti kattavamman – ja siten houkuttelevamman – palvelun tarjoamiseksi.

1.1 Tutkimusongelma ja tavoite

Tässä työssä pyrin vastaamaan kysymykseen: *Millä tavoin operaattorin kannattaa liittää eri verkoissa toteutetut leimakytkentäiset virtuaaliverkkopalvelut toisiinsa tietoturvan näkökulmasta?* Eri tapojen mielekäs vertailu edellyttää hyvin valittuja kriteereitä. Työn iso haaste onkin määritellä nämä kriteerit. Tavoitteenani on muodostaa kriteerit, jotka kattavat kaikki olennaiset MPLS-VPN-palvelut. Operaattorin valitessa sopivaa yhteenliittämistapaa sillä on muitakin huomioonotettavia seikkoja kuin tietoturvallisuus. Silloin tämän työn kriteereitä voi käyttää tietoturvaosuuden arvioinnissa.

Katson työni onnistuneeksi, jos määrittelemieni kriteerien avulla voidaan eri yhteenliittämistapojen välillä tehdä vertailu, joka osoittaa perustellusti miten ne poikkeavat toisistaan. Lisäksi työn tavoitteena on muodostaa *selkeä yleisesitys leimakytkentäisistä virtuaaliverkkopalveluista* – erityisesti autonomisten alueiden yli levittyvistä sellaisista – verkko-operaattorin näkökulmasta.

1.2 Tutkimuksen rajaus

Vertailen työssä operaattorin hallinnoimien (provisioimien) virtuaaliverkkojen liittämistä yli autonomisten alueiden rajojen. Olen käsitellyt neljä eri autonomisten alueiden yhteenliittämistapaa kolmen virtuaaliverkkopalvelun osalta. Eri virtuaaliverkkopalveluita ei verrata toisiinsa. Yhteenliittämistavoissa olen esittänyt neljä perustapausta. Kussakin yhteenliittämistavassa olen osoittanut operaattorin kannalta oleelliset ja huomioonotettavat erityispiirteet.

Tutkimuksessa olen käsitellyt seuraavia virtuaaliverkkopalveluita: "*BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot*" (BGP/MPLS IP-VPN),

"*Virtuaalijohdinpalvelu*" (VPWS) ja " *Virtuaalinen lähiverkkopalvelu"* (VPLS). Rajaus perustuu näkemyksiini ja kokemuksiini[1] olennaisimmista ja suosituimmista tekniikoista sekä operaattoreiden että laitevalmistajien keskuudessa. Näkemystäni tukee se, että suurin osa MPLS-VPN:iä koskevasta materiaalista koskee valitsemiani palveluita. Tarkemmat perustelut käsiteltävien palveluiden valintaan löytyvät alaluvusta 2.3.

Työssä pohditaan yhteenliittämistä tietoturvallisuuden kannalta. Tämä rajaus on tehty, jotta työ samaan aikaan sekä menisi riittävän syvälle tekniikassa että pysyisi hallittavan kokoisena. Tietoturva on valittu aihepiiriksi, koska se on virtuaaliverkkojen keskeinen ominaisuus.

1.3 Tutkimuksen rakenne

Tämän työn lukijalta oletetaan IP- ja MPLS-verkkojen perustoiminnan tuntemista. Näitä ovat tiedot verkkokomponenteista, niiden tehtävistä ja yleisesti käytettyjen protokollien toiminnasta.

Tästä huolimatta olen taustoittanut tutkimusongelman tässä työssä laajemmin kuin diplomitöissä on tapana. Olen katsonut tämän välttämättömäksi, sillä koko aihepiiristä (leimakytkentää hyödyntävät virtuaaliverkot) ei löydy kunnollista kokonaisesitystä suomeksi. Myöskään englanninkielisestä MPLS-VPN-kirjallisuudesta en ole löytänyt esitystä tämän työn kannalta oleellisesta, verkon sisäistä toiminnallisuutta kuvaavasta, näkökulmasta. Työn varsinaisen polttopisteen (virtuaaliverkkojen yhteenliittäminen) kannalta tilanne on vielä huonompi. Suurin osa leimakytkentää hyödyntävien verkkojen yhteenliittämistä koskevasta materiaalista on hajallaan erilaisissa epävirallisissa tilaisuuksissa pidetyissä esitelmissä (kalvoilla), joten niiden saatavuus on kyseenalainen. Edellä mainitusta syystä johtuen olen katsonut parhaimmaksi koota oleelliset perustiedot tähän työhön.

Luvussa 2 käyn läpi, miten leimakytkentä ja ennen kaikkea sitä hyödyntävät virtuaaliverkot toimivat. Luvussa esitellään BGP/MPLS IP-VPN-, VPWS- ja VPLS-palvelut ja niiden tuottaminen verkon laitteiden kannalta. Käyn läpi virtuaaliverkkopalveluiden arkkitehtuurin, komponentit ja protokollien käytön. Leimakytkentäiset virtuaaliverkot hyvin tunteva voi toisin sanoen hypätä suoraan lukuun 3.

---

[1] Olen työskennellyt operaattorin palveluksessa MPLS-VPN-asioiden parissa vuodesta 2001.

Luvussa 3 kuvaan eri toteutustavat MPLS-pohjaisten virtuaaliverkkojen yhteenliittämiseen. Kukin neljästä tavasta käydään läpi sekä yleisellä tasolla että hallintatason osalta erikseen luvussa 2 esiteltyjen palveluiden valossa.

Työn varsinainen analyysiosuus alkaa luvusta 4. Siinä määritellään vertailussa käytettävät kriteerit. Luvun alussa on kuvattuna metodi, jolla kriteerit on muodostettu. Sen jälkeen olen muodostanut kriteerit metodin mukaisesti. Kriteerien valinta perustuu kirjallisen selvityksen lisäksi käytännön työssä operaattorilla saamiini kokemuksiin. Luvun loppuun olen tehnyt taulukon, johon kriteerit on koottu. Kriteerien avulla tehty vertailu eri autonomisten alueiden virtuaaliverkkojen yhteenliittämistavoista on luvussa 5. Vertailu on teoreettinen, koska eri verkkojen rakentaminen ei ollut mahdollista. Olen pohtinut vertailun tuloksia luvun 5 yhteenvedossa ja laajemmin liitteessä A.

Johtopäätöksissä (luku 6) pohdin työlle asetettujen tavoitteiden toteutumista, vertailun tuloksia ja kriteerien onnistuneisuutta. Yhtenä menetelmänä tässä on pohdinta siitä, missä eri yhteenliittämistapoja voisi soveltaa. Samassa luvussa pohdin myös avoimeksi jääneitä asioita ja mahdollisia tulevaisuuden tutkimuksen kohteita tutkimuksen aihepiiriin liittyen.

luku 2:
Leimakytkentä ja sitä hyödyntävät virtuaaliverkkopalvelut

Tässä luvussa käsitellään leimakytkentää (MPLS) ja erityisesti sen tämän työn kannalta tärkeintä sovellusta: virtuaaliverkkopalveluita (MPLS-VPN:t). Leimakytkennästä itsestään on ollut saatavilla hyvää kirjallisuutta jo vuosia ja materiaalia suomeksikin. Alaluvussa 2.1 on lyhyesti kerrattu leimakytkennän olennaiset puolet tämän työn kannalta, mutta kokonaisesitykseksi aiheeseen siitä ei ole. Leimakytkentäisistä virtuaaliverkkopalveluista olen tehnyt kattavamman esityksen (loput alaluvut). Teknisten yksityiskohtien läpikäyminen on välttämätöntä, sillä juuri yksityiskohtien eroihin perustuvat mahdollisuudet kontrolloida sekä virtuaaliverkkopalveluita yleensä että niiden yhteenliittämistä yli verkko- ja operaattorirajapintojen erityisesti.

Työssä tarkastellaan eri virtuaaliverkkopalveluiden yhteenliittämisen vaikutuksia MPLS-VPN-operaattorille ja -asiakkaille. Tässä luvussa käydään läpi kolme eri virtuaaliverkkopalvelua tästä näkökulmasta. Virtuaaliverkkopalveluiden tarjoamat palvelut asiakkaiden suuntaan ovat työn kannalta sivuroolissa, joten niitä ei kattavasti käsitellä, eikä työtä kannata käyttää näiden palveluitten tai niiden erojen yksityiskohtaiseen ymmärtämiseen.

Valitut virtuaaliverkkopalvelut esitellään toiminnallisesta näkökulmasta: mitä toimintoja virtuaaliverkkopalvelualustan (runkoverkon) pitää toteuttaa, jotta operaattori voi sen avulla tarjota käsiteltyjä virtuaaliverkkopalveluita; missä verkkolaitteissa nämä ominaisuudet voi toteuttaa; mitä tietoja verkkolaitteiden välillä kulkee ja minkä protokollien avulla tätä tietoa levitetään; ja mitkä mahdollisuudet operaattoreilla on kontrolloida tätä kaikkea. Näitä ominaisuuksia tullaan peilaamaan virtuaaliverkkopalveluiden yhteenliittämisen näkökulmasta luvussa 3.

Alaluvussa 2.2 käydään läpi virtuaaliverkon määritelmä ja standardoinnin tämänhetkinen tilanne. Alaluvussa 2.3 on perusteltu, miksi juuri valitut virtuaaliverkkopalvelut on otettu tarkasteluun. Tämän jälkeen paneudutaan valittuihin virtuaaliverkkopalveluihin kuhunkin omassa alaluvussaan. Jokaisen

virtuaaliverkkopalvelun erittelyn jälkeen olen koonnut tämän työn - eri verkoissa toteutettavan palvelun - kannalta olennaisimmat seikat yhteen.

Leimakytkentään perustuvat virtuaaliverkkopalvelut on esitetty joko suppeasti vain yhtenä MPLS-tekniikan sovelluksena, kuten kirjoissa "MPLS and VPN Architectures" [Gui01] ja ” MPLS and VPN Architectures Vol. 2” [Pep03] tai vain yhtenä VPN:n toteutustapana muiden joukossa (korostaen "asiakasnäkökulmaa"; mitä VPN-palvelu tarjoaa asiakkaalle). Tähän mennessä ainoita opinnäytetöitä MPLS-VPN:istä Suomen korkeakouluissa ja yliopistoissa on Harri Välimäen ”Leimakytkentää hyödyntävien virtuaaliverkkojen vertailu” [Väl02], tämän lisäksi Juha Rahikainen on tehnyt Jyväskylän ammattikorkeakoulussa opinnäytetyön ”MPLS-liikenteen tietoturva” [Rah06], jossa sivutaan MPLS-VPN:ien tietoturvaa. Välimäen diplomityössä verrataan *eri virtuaaliverkkopalveluita keskenään yhden operaattorin verkkoympäristössä.* Tässä työssä ei vertailla eri palveluita keskenään, vaan vertaillaan *samojen virtuaaliverkkopalveluiden eri toteutustapoja monen operaattorin ympäristössä.* Välimäen diplomityössä ollaan kiinnostuneita siitä, mitä tapahtuu reunareitittimissä ja niistä asiakaslaitteisiin päin, kun taas tässä työssä *mielenkiinto on nimenomaan reunareitittimien välisessä toiminnassa*. Rahikaisen työssä keskitytään käsittääkseni[2] simuloinnin avulla siihen, minkälaisia tietoja tunkeutuja voi saada reitittimestä, eikä niinkään itse MPLS-VPN-tekniikan toimintaan. Internetistä - lähinnä reititinlaitevalmistajien sivuilta - löytyy eritasoisia papereita (White papers) aihetta sivuten, mutta niissäkin tieto on usein sekä valmistajakohtaista että hajanaista, joten olen katsonut parhaimmaksi tehdä tämän luvun kootakseni tarvittavat tiedot yhteen paikkaan aihetta jäsentämään.

2.1 Yleistä leimakytkennästä

Leimakytkentä on määritelty IETF:n dokumentissa *Multiprotocol Label Switching Architecture* [Ros01a]. Dokumentissa on esitelty monia tapoja toteuttaa leimakytkentää. Näistä vain osa on nykyisin käytössä. Tässä alaluvussa on keskitytty näihin nykyisin käytössä oleviin ja niistäkin vain asioihin, jotka ovat virtuaaliverkkopalveluiden ja tässä työssä käsitellyn tietoturvan kannalta olennaisia[3].

MPLS-verkon hallintataso perustuu liikenteen kytkentätavasta riippumatta IP-protokollan ja -osoitteiden käyttöön. Tässä työssä leimakytketty verkko on

---

[2] Arvio Rahikaisen opinnäytetyöstä on tehty abstraktin perusteella.

[3] Käypä katsaus leimakytkentätekniikan perusteisiin on esimerkiksi professori Raimo Kantolan luentokalvot (jo vuodelta 1999!) [Kan99]. Laajemmin aiheesta on esimerkiksi kirjassa [Dav00].

pakettiverkko, jossa pakettikytkennässä hyödynnetään dokumentin *MPLS Label Stack Encoding* [Ros01b] määrittelemää MPLS-otsaketta (*engl. "shim" header*), eikä esimerkiksi ATM-verkon VCI/VPI-arvoja.

MPLS:n ja sen edeltäjien tavoitteena oli ensisijaisesti nopeuttaa pakettikytkentää ja tehdä sen viiveistä ennustettavampia käyttämällä verkko-osoitteiden sijasta kiinteänmittaisia numeroita eli leimoja (*engl. label*) liikenteen välittämisen apuna [Rag02]. Vaikka reititinten kehityksen myötä tämä seikka on menettänyt merkityksensä, sen tietäminen auttaa ymmärtämään MPLS:n toimintafilosofiaa ja sitä kautta MPLS:n toimintaa ja rajoituksia.

2.1.1 Leimaverkon laitteet

Leimakytkeviä reitittimiä kutsutaan leimareitittimiksi tai LSR:ksi[4] (*engl. Label Switching Router*). Leimaverkon reunalla olevaa reititintä, joka välittää leimatonta liikennettä leimakytkettyyn verkkoon ja liikennettä leimaverkosta leimattomaan, kutsutaan leima-alueen reunareitittimiksi eli LER:ksi (*engl. Label Edge Router*). Koska MPLS:n hallinta perustuu IP:hen, ovat kaikki leimareittitimet IP-reitittimiä, vaikka välittäisivät vain leimakytkettyä liikennettä.

Leimakytkettyjen virtuaaliverkkojen yhteydessä käytetään LSR:n ja LER:n sijasta hieman erilaisia nimityksiä P ja PE. Nämä nimitykset eivät täysin vastaa LSR:ää ja LER:ää. Nämä käsitteet esitellään VPN-palveluiden yhteydessä alaluvussa 2.4.

2.1.2 Leima, leimatut paketit ja niiden kytkentä

Leimat voi mieltää kahden leimareitittimen väliseksi "sopimukseksi", että ylävirrassa[5] oleva leimareititin R_u lähettää alavirrassa olevalle leimareitittimelle R_d kaikki paketit, jotka kuuluvat samaan ryhmään, samalla tunnisteella (= leimalla) varustettuna. R_d osaa siten kohdella näitä paketteja samoin pelkästään tuota tunnistetta tutkimalla. Ryhmää paketteja, joita on tarkoitus kohdella samoin tietyssä osassa verkkoa, kutsutaan kytkentäluokaksi (FEC, *engl. Forwarding Equivalence Class*). Tapa, jolla

---

[4] Joissain yhteyksissä (esim. [Kan99]) on esiintynyt myös lyhenne LR, mutta selkeyden vuoksi käytän joko koko suomenkielistä nimeä leimareititin tai sitten vakiintunutta englanninkielistä lyhennettä LSR.

[5] Yhdensuuntaisessa liikenteessä ylävirran laitteeksi sanotaan laitetta, joka lähettää paketin alavirran laitteelle. Käsite riippuu siis liikenteen suunnasta ja kahdensuuntaisessa liikenteessä samat laitteet ovat vastakkaisissa rooleissa eri liikennesuuntien suhteen.

leimareitittimet jakavat ymmärryksen leimoista ja kytkentäluokista, riippuu sekä leimojen levitystavasta, että IP-reitityksestä. [Ros01a]

Leimojen arvot ovat ”vain” numeroita, eikä niihin ole koodattuna minkäänlaista osoiteinformaatiota tai tietoa niiden käyttötarkoituksesta. Lukuun ottamatta tiettyjä varattuja leima-arvoja, reititin voi vapaasti päättää, mitä leima-arvoja se käyttää mihinkin tarkoitukseen[6][And01]. Toisin sanoen leiman myöntäjä (R_d) voi käyttää mitä tahansa arvoa mille tahansa kytkentäluokalle, kunhan leimanaapuri (R_u) saa tästä tiedon. Käytännössä leimojen arvot eivät ole mielivaltaisia, vaan riippuvat reititinvalmistajan toteutuksesta [Beh07]. Tällä seikalla on merkitystä leimoja väärennettäessä, jolloin valistuneella arvauksella on todennäköisempää löytää käytetty leima.

Leimat ovat paikallisia: niillä on merkitystä vain leiman myöntäjälle R_d, joka tekee sen perusteella päätöksiä paketin kohtelusta, ja tämän naapurille ylävirrassa R_u, jonka tulee osata lisätä tai vaihtaa se tiettyyn kytkentäluokkaan kuuluvaan pakettiin [Ros01a]. Samaa leiman arvoa voi käyttää toisessa yhteydessä aivan toiseen tarkoitukseen. Tämä lisää leimaverkkototeutusten skaalautuvuutta.

Paikallisesti leimoja voi allokoida kahdella eri tavalla: niin, että samat leimat ovat yksikäsitteisiä koko reitittimessä (*engl. Per-platform label space*) tai niin, että ne ovat liitäntäkohtaisia (*engl. Per-interface label space*). Edellä mainittu tarkoittaa sitä, että paketti tulkitaan vain leimansa perusteella riippumatta liitännästä, josta se tulee sisään. Jälkimmäinen sitä, että paketin kohtelu riippuu leiman lisäksi liitännästä, josta se tulee sisään. Reititinkohtaiset leimat käyttävät resursseja tehokkaammin ja mahdollistavat nopean vikapaikan ohituksen FRR-toiminteen (*engl. Fast Reroute*) avulla. Liitäntäkohtaiset leimat ovat tiukemmin hallittuja ja tästä syystä tietoturvallisempia. Käytännössä liitäntäkohtaisia leimoja käytetään ainoastaan silloin kun ATM:n VCI/VPI-arvoja käytetään leimoina [Luo05].

Vaikka leimoilla sinänsä on merkitystä vain paikallisesti, paketeille muodostuu niiden avulla reittejä verkon läpi, joissa pakettien välitys perustuu ainoastaan leimakytkentään. Näitä reittejä kutsutaan leimapoluiksi (LSP, *engl. Label Switched Path*). Samaan kytkentäluokkaan kuuluvat paketit kulkevat samaa leimapolkua pitkin. [Ros01a]

---

[6] Joissakin toteutuksissa tämä on joko käyttäjän konfiguroitavissa tai ennalta määrätty (reitittimen ohjelmistossa), mutta standardi ei rajaa eri leima-avaruuksien käyttötarkoituksia.

Usein LSP:t menevät koko verkon läpi reunalta toiselle, mutta niitä voi olla myös kahden LSR:n välillä. Tällaisia polkuja käytetään esimerkiksi, jotta verkossa olisi nopea varareitti käytössä linkkien tai solmupisteiden hajoamisen sattuessa. [Swa05]

Paketilla voi olla useampia leimoja ”pinossa” (*engl. label stack*). Tämä mahdollistaa hierarkkisen reitityksen (LSP:t toisten LSP:iden sisällä), sillä normaalisti vain ulointa (”päällimmäistä”) leimaa käytetään kytkentäpäätöksen tekoon. Sisempää leimaa käytetään vasta ulomman leiman osoittaman leimapolun päätepisteessä.[Ros01a]

MPLS-otsakkeella varustettu paketti voi kuljettaa mitä tahansa dataa, joka soveltuu kuljetettavaksi pakettiverkon yli: paketeilla ei tarvitse olla IP-otsaketta. Toisaalta, vaikka leiman alla olisi IP-otsake, ei leimareitittimen tarvitse osata reitittää sitä (= ymmärtää sen osoitteistusta): riittää, että leimareititin osaa kytkeä sen paketin leiman perusteella [Ros01a]. Nämä ominaisuudet ovat erityisen hyödyllisiä virtuaaliverkkopalveluille.

2.1.3 Leimojen levitys ja siihen käytetyt protokollat

Leimareitittimet käyttävät yleensä reititysprotokollaa verkon topologiainformaation selvittämiseksi. Tämä on välttämätöntä, jos leimoja halutaan signaloida jonkin dynaamisen protokollan avulla[7]. Protokollat, joita voidaan käyttää leimojen mainostamiseen, ovat:

- LDP-protokolla (*engl. Label Distribution Protocol*) [And01] ja sen laajennus CR-LDP (*engl. Constraint-Based LSP Setup using LDP*) [And02]
- RSVP-protokolla (*engl. RSVP-TE: Extensions to RSVP for LSP Tunnels*) [Awd01]
- BGP-protokolla (*engl. Carrying Label Information in BGP-4*) [Rek01]

Näistä kaksi ensin mainittua hyödyntävät IGP-protokollien reititysinformaatiota ja BGP:ssä leimainformaatio taas on lisätty laajennuksen avulla normaaliin reitityssanomaan. Leimoja välitetään myös virtuaaliverkkojen palvelusignaloinnissa. Käytännössä niissä käytetään laajennettuja versioita LDP:stä ja BGP:stä.

LDP:n toimintamalli on ”avoin”: sitä käytettäessä leimareititin jakaa automaattisesti[8] leimat kaikille verkkosuunnille (prefixeille), joita se IGP:ssäkin mainostaa. RSVP:tä

---

[7] Staattisten leima-arvojen käyttö on mahdollista. Tällöin myös topologia-informaatio voidaan kerätä staattisesti.

[8] Leimamainostuksia voidaan erikseen rajoittaa haluttaessa.

käytetään haluttaessa tehdä liikenteen hallintaa (TE, *engl. Traffic Engineering*). Sen toimintamalli on ”suljettu”: leimareititin ei signaloi leimoja kaikille kaikkiin verkkosuuntiin, vaan vain niille poluille ja verkkosuunnille, joita halutaan käytettävän. LDP:llä muodostuu leimapolkuja, jotka noudattavat IGP:n osoittamaan ”parasta[9]” reittiä. RSVP:llä voidaan signaloida käytettäväksi muitakin reittejä. BGP:n toimintamalli on samantapainen LDP:n kanssa, mutta BGP:n mainostamia reittejä hallitaan yleensä niin tarkoin, että avoimuus on sen yhteydessä ehkä hieman harhaanjohtava ilmaus. [And01][And02][Awd01][Rek01]

Leimattujen pakettien kytkentä ei riipu siitä, millä protokollalla leimat on signaloitu. Kytkentäpäätöstä tehtäessä leimareititin konsultoi kytkentätaulua, jossa eri tavoin signaloiduilla leimoilla ei ole eroa.

2.1.4 Leimakytkennän turvallisuus

Leimakytkentä ei sinällään ole sen turvallisempi tai turvattomampi kuin IP-osoitteisiin perustuva kytkentä. Molemmissa on syytä huolehtia sekä solmupisteiden (reititinten) että yhteyksien (linkkien) turvallisuudesta. Normaalit reititinten suojaamiskeinot pätevät myös leimareitittimiin ja leimaprotokollat ovat autentikoitavissa siinä kuin reitityksprotokollatkin. [Beh05]

Leimakytkentä mahdollistaa runkoverkon piilottamisen hieman helpommin kuin tavallinen IP-verkko. Tämä voidaan toteuttaa liittämällä kaikki ulkopuoliset yhteydet virtuaaliverkkoihin [Beh05]. Tällöin runkoverkossa voidaan käyttää haluttaessaa yksityistä IP-osoiteavaruutta. Piilotetun runkoverkon riskinä on, että palveluista tulee monimutkaisia toteuttaa. Monimutkaisuus taas lisää väärin konfiguroinnin riskiä, joka puolestaan on tietoturvariski. Tältä osin MPLS:n turvallisuus on siis painotuskysymys.

MPLS:n turvallisuuteen liittyy riski, joka johtuu sen historiasta: sitä on kehitetty yhden operaattorin verkossa toimivaksi tekniikaksi. Tämä näkyy sekä standardoinnissa (sen puutteessa) liittyen inter-AS-toteutuksiin että erityisesti laitevalmistajien MPLS-toteutuksissa. Konkreettinen esimerkki tästä on reititinkohtaisen leima-avaruuden käyttö. Sen takia leimojen avulla ei voi tehdä liitäntäkohtaista suodatusta[10]. Verkossa, jossa kaikki leimanaapurit oletetaan yhtä

[9] CR-LDP:n puitteissa ”paras” voi olla muutakin kuin alhaisimman IGP-metriikan omaava, mutta silti se on annetuilla kriteereillä ”paras”.

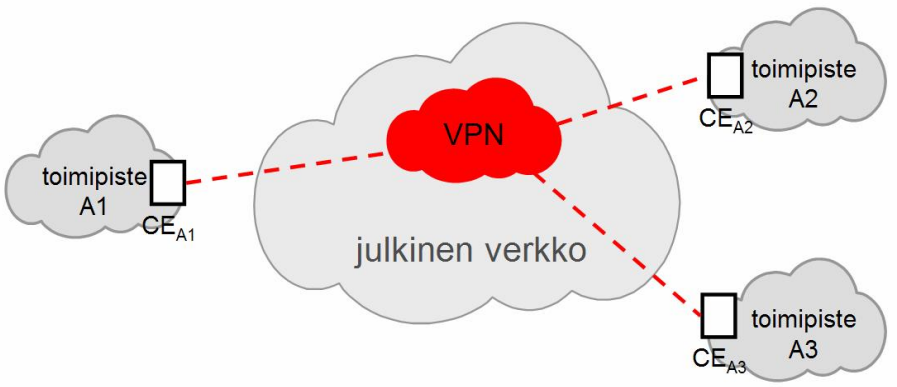
[10] Näin on ainakin Cisco systemsin tämän hetken toteutuksissa. [Beh07]

turvallisiksi, leimojen perusteella suodatus olisi ollut vain lisärasite reitittimelle[11]. Operaattorien välisissä yhteyksissä liikenteen suodatusmahdollisuus on itsestään selvä ominaisuus.

2.2 Yleistä virtuaaliverkoista

2.2.1 Mikä on virtuaaliverkko?

Virtuaaliverkko (VPN, *engl. Virtual Private Network*) on löyhästi määriteltynä tiedonsiirtoverkko, jossa asiakkaan toimipisteiden väliset yhteydet on toteutettu käyttäen jaettua infrastruktuuria ja jolla on samat pääsy- ja turvallisuuskäytännöt kuin yksityisellä verkolla [Gui01]. VPN toisin sanoen muodostaa julkiseen verkkoon suljetun käyttäjäryhmän, jonka on mahdollista viestiä keskenään yksityisesti. Virtuaaliverkkopalvelulla tarjotaan virtuaaliverkko haluttujen asiakkaan toimipisteiden välille (kuva 1) tai yleisemmin minkä tahansa haluttujen elementtien välille verkossa. Virtuaaliverkko on helpointa mieltää asiakassovelluksena, mutta sen lisäksi operaattori voi käyttää VPN:iä myös esimerkiksi erottamaan palveluita toisistaan, kuten ajaa puheliikennettä yhdessä virtuaaliverkossa ja Internet-liikennettä toisessa.



Kuva 1. Virtuaaliverkko on yhdistämispalvelu

2.2.2 Leimakytkentäisten virtuaaliverkkopalveluiden standardoinnista

Tärkein Internet-tekniikoita standardoiva elin on Internet Engineering Task Force (IETF). Tämän lisäksi YK:n alainen tietoliikennealan standardointi- ja kehitysjärjestö

[11] Reitittimen suorituskykyä olennaisempaa on varmasti se, ettei tällaiseen ”turhaan” ominaisuuteen ole nähty syytä laittaa tuotekehityspanoksia.

ITU-T on viime vuosina antanut suosituksia myös Internet-toimialueella. IETF:n ja ITU-T:n roolijako ei ole selkeä, mutta MPLS-VPN:ien osalta kaikki tekniset standardit tehdään IETF:n puitteissa. Sen sijaan esimerkiksi arkkitehtuuri- ja palvelukuvauksia tunnutaan tekevän molemmissa. Karkeasti voi sanoa, että ITU-T:n tekemät dokumentit ovat vain selkeytettyjä kuvauksia IETF:n varsin sekavasta dokumenttijoukosta. Tämä tekee niistä selkeämmin hallittavia, mutta toisaalta ne eivät suhteellisen helppolukuisuutensa lisäksi tarjoa varsinaista omaa sisältöä. Harmittavasti ITU-T:n käyttämä terminologia poikkeaa jonkin verran IETF:n käyttämästä terminologiasta. Kun tähän lisää vielä sen, että IETF:n dokumenteissa käytetty terminologia ei ole yhtenäinen, niin dokumenteissa käytetty sanasto on hyvin kirjavaa. IETF:n puitteissa sanastoa on yritetty yhtenäistää [Aug06], mutta tämä ei auta ennen suositusta julkaistuihin dokumentteihin.

IETF on organisaationa hajanainen ja vain löyhästi järjestäytynyt, mistä johtuen sen standardointiprosessi on monivaiheinen ja hidas [Bra96]. IETF:n työ on kuitenkin monia muita standardointiorganisaatioita selkeästi enemmän keskittynyt konkreettisten ongelmien ratkaisemiseen, mikä on ollut sen etu nopeasti kehittyvissä Internet-teknologioissa. Edellä mainitusta seuraa, että IETF tuottaa paljon ratkaisuja erilaisiin ongelmiin, mutta näitä ratkaisuja ei usein saada standardoitua[12] ja lisäksi eri ratkaisut ovat välillä huonosti keskenään koordinoituja. Laitevalmistajat ja operaattorit toteuttavat tuotteitaan kuitenkin riippumatta tekniikoiden virallisesta standardiasemasta. Usein riittää, että ”standardi” on dokumentoitu IETF:n standardointiprosessina pysyvänä dokumenttina, RFC:nä (*engl. Request for Comments*) tai jopa IETF:n tilapäisenä työdokumenttina, ns. Internet-draftina. Operaattorin kannalta tällaisilla "standardeilla" on standardien merkittävimmät hyvät ominaisuudet: ne ovat julkisia, kaikkien laitevalmistajien toteutettavissa olevia – ja toivon mukaan myös selkeästi määriteltyjä ja yhteensopivia toteutuksia tuottavia. Toisin sanoen, ne pienentävät operaattorin riskejä liittyen yhteen laitevalmistajaan sitoutumiseen tai yhteensopimattomuuteen muiden laitevalmistajien, operaattoreiden tai asiakkaiden kanssa.

IETF:ssä on kaksi työryhmää, jotka standardoivat *operaattoreiden hallinnoimia* (*engl. provider-provisioned*) virtuaaliverkkoratkaisuja. Työryhmistä *Layer 3 Virtual Private Networks* (L3vpn) keskittyy virtuaaliverkkoratkaisuihin, joilla operaattorit voivat tarjota asiakkaille verkkokerroksen (OSI-mallin mukainen kolmas kerros)

[12] Monet tärkeät, Internetissä ja muissa Internet-tekniikkaa hyödyntävissä verkoissa laajasti käytetyt, tekniikat eivät ole vuosien saatossa saaneet virallista Internet Standardin statusta; tästä esimerkkinä Border Gateway Protocol -protokolla (BGP-4) ja Leimakytkentä (MPLS). [Iet07d]

virtuaaliverkkopalvelun. Käytännössä L3vpn:n on standardoinut vain IP-protokollaa tukevia virtuaaliverkkoja. *Layer 2 Virtual Private Networks* (L2vpn) -työryhmä keskittyy ratkaisuihin, joilla operaattorit voivat tarjota asiakkailleen siirtoyhteyskerroksella (OSI-mallin mukaisella toisella kerroksella) toimivia virtuaaliverkkoja läpi operaattorin verkon. Näiden kahden työryhmän lisäksi työryhmä *Pseudo Wire Emulation Edge to Edge* (Pwe3) standardoi emuloinnin avulla toteutettuja näennäisjohtimia verkon reunalta toiselle. Kaikissa kolmessa edellä mainitussa työryhmässä MPLS-tekniikalla on keskeinen, joskaan ei pakollinen, rooli verkkotason tekniikkana. Kaikki niiden standardoimat palvelut on standardoitu ensisijaisesti käyttämään MPLS:ää, mutta muita tunnelointitekniikoita ei ole suljettu pois.

L3vpn-työryhmä aikoo standardoida kolme palvelua: *BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot* (*engl. BGP/MPLS IP Virtual Private Networks (VPNs)*), *Virtuaalireitittimiin perustuvat IP-virtuaaliverkot* (*engl. IP VPNs using Virtual Routers*) ja *Asiakasreitittimiin perustuvat, IPseciä hyödyntävät virtuaaliverkot* (*engl. CE-based VPNs using IPSEC*) [Iet06]. L2vpn-työryhmä aikoo myös standardoida kolme eri palvelua: *Virtuaalinen lähiverkkopalvelu* (VPLS, *engl. Virtual Private LAN Service*), *Virtuaalijohdinpalvelu* (VPWS, *engl. Virtual Private Wire Service*) ja *Vain IP-paketteja kuljettava virtuaaliverkkopalvelu* (*engl. IP-only VPNs*) [Iet07a]. Viimeksi mainittu tunnetaan myös nimellä *IP-Only LAN Service* (IPLS) [Sha06]. Pwe3-työryhmän ei ole tarkoitus määritellä palveluita, vaan keskittyä virtuaalijohdinten teknisen toteuttamisen määrittelyyn. L2vpn hyödyntää Pwe3:n määrittelyjä omien palveluidensa pohjana.

Tällä hetkellä IETF on julkaissut pysyvät dokumentit (RFC:t) osasta edellä mainituista palveluista, muttei kaikista. L3vpn on julkaissut palvelusta *BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot* ensin RFC:n 2547 ja myöhemmin tämän päivitetyn version RFC 4364. RFC 4364:ää on myös tarkennettu ja sen kattavuutta on laajennettu joukolla muita RFC:itä. Toistaiseksi L3vpn ei ole julkaissut kahteen muuhun palveluunsa liittyviä RFC:itä, mutta näistä keskeneräistä on julkaistu joukko Internet-drafteja. RFC 4364 oli pitkään työstettävänä, mistä syystä uudistettuun standardiin viitataan edelleen usein työnimellä "RFC2547bis".

L2vpn on julkaissut VPLS-palvelusta kaksi kilpailevaa dokumenttia, muiden palveluiden osalta tilanne on epäselvempi[13]. Kilpailevien VPLS-palveluiden suurin ero

---

[13] Sekä VPWS että IPLS on toiminta on kuvattu, muttei määritelty kehysdokumentissa "*Framework for Layer 2 Virtual Private Networks (L2VPNs)*" [And06]. IPLS:stä löytyy myös Internet-Draft ”*IP-Only LAN Service (IPLS)*”, jota tosin ei ole päivitetty kymmeneen kuukauteen.

on käytetty signalointiprotokolla: RFC 4761 perustuu BGP:n käytölle ja RFC 4762 LDP:n käytölle. Yksittäisten standardien tilanteesta ajantasaisimman kuvan saa IETF:n veppisivuilta (http://www.ietf.org/).

ITU-T on julkaissut ”*Global information infrastructure and internet protocol aspects*”-sarjassaan (Y-sarja) muutamia virtuaaliverkkoja ja muutamia MPLS:ää koskevia dokumentteja. Dokumentit kirjaavat virtuaaliverkkopalveluiden yleisiä vaatimuksia ja esittelevät erilaisia verkkoarkkitehtonisia lähestymistapoja näiden toteuttamiseksi. ITU-T:n standardointi ei tällä hetkellä vaikuta virtuaaliverkkopalveluiden toteutuksiin[14], joten en ole käsitellyt niitä tarkemmin.

2.3 Työssä käsitellyt virtuaaliverkkopalvelut

Tässä työssä käsittelen vain osaa ehdotuksista virtuaaliverkkopalvelustandardeiksi. Olen rajannut monia palveluehdotuksia tarkastelun ulkopuolelle, koska en usko niiden olevan operaattorien kannalta merkityksellisiä; pitääkseni työn hallittavan kokoisena; tai koska niistä ei ole riittävästi materiaalia saatavilla. Merkityksellisyyden operaattorien kannalta perustan kolmeen seikkaan: 1. useamman vuoden työkokemukseeni aihepiirin parissa teleoperaattorilla, 2. isoimpien reititinvalmistajien (Cisco systems ja Juniper networks) julkaisemaan materiaaliin ja tukemiin tekniikoihin liittyen virtuaaliverkkopalveluihin ja 3. MPLS-foorumin yhteistoimintatestien piiriin otettuihin palveluihin. Materiaalin vähyydestä osoituksena on se, ettei niistä ole julkaistu pitkäikäisiä Internet-drafteja[15].

Muut kuin runkoverkossa toteutetut palvelut on myös rajattu tämän tarkastelun ulkopuolelle, vaikka operaattorit voivat tarjota myös tällaista asiakaslaitteiden avulla toteutettua virtuaaliverkkopalvelua. Asiakaslaitteiden avulla toteutetut virtuaaliverkot vastaavat runkoverkon kannalta vaatimuksiltaan normaalia internetpalvelua, eivätkä aseta operaattorirajapinnalle mitään erityisiä vaatimuksia. Tässä työssä käsitellään siis PE- eikä CE-pohjaisia VPN-palveluita.

MFA forumin (entinen MPLS forum) puitteissa testataan leimakytkentää hyödyntäviä virtuaaliverkkotekniikoita yhteensopivuuden takaamiseksi eri laitevalmistajien kesken.

---

[14] ITU-T:n asema on perinteisesti ollut heikko IETF:n hallitsemilla pakettiverkkotekniikoiden alueella. Y-sarjan dokumentit ovat haettavissa Internetistä <http://www.itu.int/rec/T-REC-Y/>.

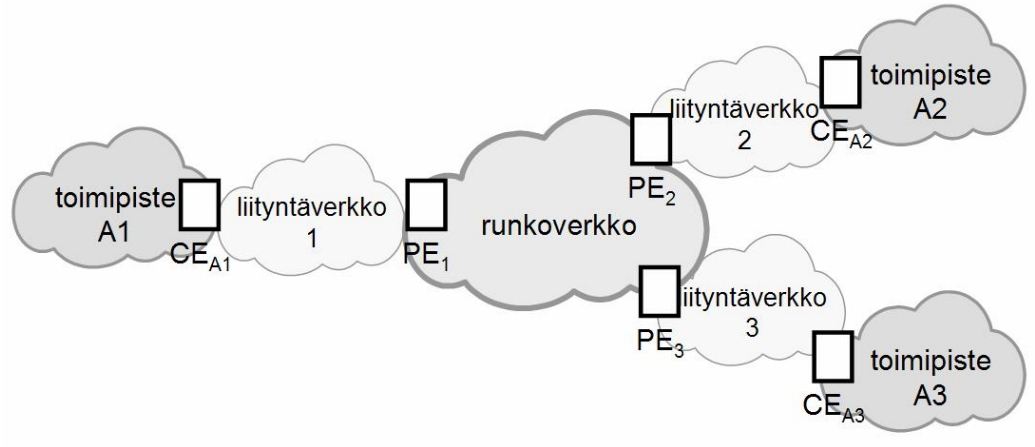
[15] Internet-draftien pitkäikäisyys tarkoittaa, että niistä on julkaistu useampia versioita, joka puolestaan tarkoittaa, että ne on katsottu kehittämisen arvoisiksi. Päivittämättömien Internet-draftien elinaika on maksimissaan kuusi kuukautta. [Bra96]

Tällä hetkellä MFA forumin puitteissa on nähty tärkeäksi testata *BGP-protokollaa ja leimakytkentää hyödyntäviä IP-virtuaaliverkkoja*, *L2-virtuaalijohtimia* ja *Virtuaalista lähiverkkopalvelua* [Ros07]. Nämä kolme tekniikkaa ja palvelua ovat ne, joihin tässä työssä keskitytään.

Seuraavaksi siirryn käsittelemään itse virtuaaliverkkopalveluita ja niiden toteutustapoja. Luvussa 2.4 esitellään kaikille työn virtuaaliverkkopalveluille yhteisiä piirteitä, tämän perässä kolme esiteltyä virtuaaliverkkopalvelua ovat omissa alaluvuissaan: alaluvussa 2.5 palvelu "BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot", alaluvussa 2.6 Virtuaalijohdinpalvelu ja alaluvussa 2.7 Virtuaalinen lähiverkkopalvelu. Tämän luvun viimeisessä alaluvussa 2.8 on lyhyesti koottuna kaikkien kolmen palvelun olennaiset piirteet liittyen useamman autonomisten alueen kattavan palvelun luomiseen.

2.4 MPLS ja virtuaaliverkkopalvelut

Kuvassa 2 on esitelty kaikille tässä työssä käsitellyille virtuaaliverkkopalveluille yhteiset osat. Alla olevassa taulukossa 1 on kirjoitettu auki näiden osien roolit. [Aug06][And06][Cal05]



Kuva 2. VPN-palvelun toteutuksen verkot ja näitä yhdistävät laitteet

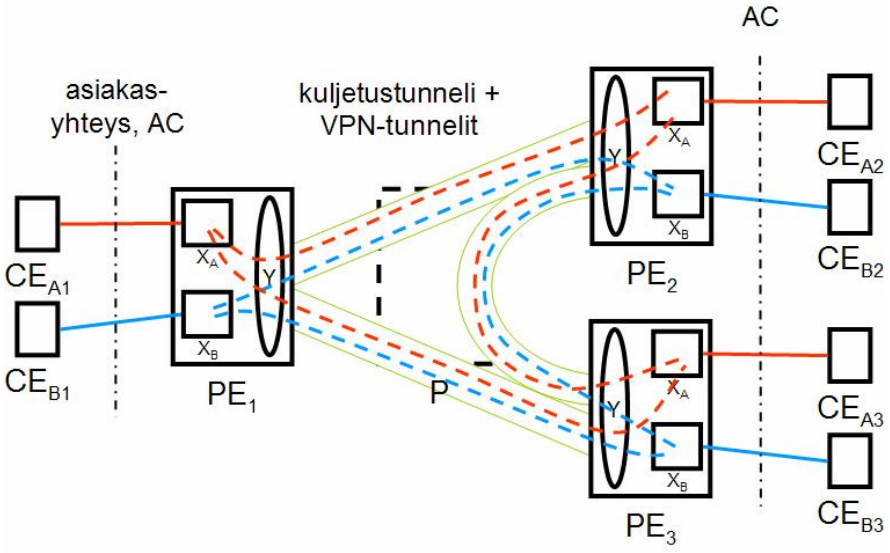
Taulukko 1 Palvelun toteutuksen verkot ja näitä yhdistävät laitteet

Toimipiste (*engl. site*): Toimipiste voidaan ajatella paikallisena verkkona, jolla on keskinäiset yhteydet ilman virtuaaliverkkoa. Toimipisteet ovat kokonaisuuksia, jotka virtuaaliverkkopalvelun avulla liitetään yhteen. Toimipiste on usein lähiverkko, mutta voi yhtä hyvin olla esimerkiksi yksittäinen työasema. Virtuaaliverkkopalvelussa on vähintään kaksi toisiinsa liitettävää toimipistettä.
CE-laite (*engl. Customer Edge device*): CE-laite on toimipisteen laite, jolla se kytkeytyy operaattorin runkoverkon reunalaitteeseen (PE-laite). CE-laite on usein reititin, mutta voi olla myös esimerkiksi Ethernet-kytkin taikka työasema. CE:llä ei ole "tietoa" VPN-palvelusta, vaan virtuaaliverkko näyttää CE:lle samalta kuin verkko tai yhteys, jota virtuaaliverkkopalvelu ”matkii”.
Liityntäverkko (*engl. Access Network*): Liityntäverkon avulla asiakkaan CE-laite liitetään operaattorin PE-laitteeseen. Tekniikaltaan se voi minimissään olla vain johdin CE- ja PE-laitteiden välillä, mutta yhtä hyvin se voi olla esimerkiksi Metro-Ethernet-verkko. Liityntäverkko voi olla myös virtuaalinen – esimerkiksi Internetin läpi tunneloitu yhteys.
PE-laite (*engl. Provider Edge device*): PE-laite on operaattorin runkoverkon laite, johon virtuaaliverkkopalvelun asiakas on liittyneenä. Yleensä PE-laite on operaattorin leimakytketyn runkoverkon reunareititin. Virtuaaliverkkopalvelu toteutetaan vain niissä PE-reitittimissä, joihin virtuaaliverkkopalvelulla yhdistettävät toimipisteet ovat kytkettyinä, muille reuna- ja runkoreitittimille virtuaaliverkkopalvelut eivät näy[16].
Runkoverkko (*engl. Provider Network(s)*): Runkoverkko on se verkko (tai ne verkot), jotka yhdistävät PE-laitteet toisiinsa. PE-laitteet käyttävät runkoverkkoa sekä VPN-liikenteen kuljettamiseen että kommunikointiin keskenään. Jos runkoverkko koostuu useammasta verkosta, tarvitaan operaattorilta erikoisjärjestelyjä, tähän palataan luvussa 4 (Tämän työn varsinainen aihe!).
P-reititin (*engl. Provider (core) router*): Kuvasta on jätetty pois runkoverkon leimakytkevät P-reitittimet. P-reitittimeen ei ole liitettynä CE-laitteita, eikä sillä ole mitään VPN-kohtaista tilatietoa. P-reitittimet ovat kuitenkin oleellinen osa virtuaaliverkkopalveluita, sillä niiden avulla PE-reitittimillä on yhteydet toisiinsa. P-reititin kohtelee VPN-paketteja samoin kuin kaikkia muitakin MPLS-paketteja (ainoastaan uloimman leiman perusteella).
ASBR-reititin (*Autonomous system border router*)(ei näy kuvassa): ASBR on runkoverkon reititin, joka on liittyneenä kahteen tai useampaan autonomiseen alueeseen. ASBR:llä on erityistehtäviä luotaessa useamman autonomisen alueen kattava VPN-palvelu. Tästä lisää luvussa 3, jossa käsitellään VPN-toteutuksia AS-rajapinnan yli

[16] Reunareitittimien lisäksi myös reittiheijastinta (RR), reittikeskitintä (VPLS-hub) ja tiettyjä verkon palveluita (kuten DNS ja RADIUS) käytetään tietyissä toteutuksissa.

2.4.1 Leimakytkentää hyödyntävien virtuaaliverkkojen referenssimalli

Kuvassa 3 on esitetty edellisen kuvan tapaus hieman muokattuna (siihen on lisätty P-reititin sekä toinen asiakas ja tämän virtuaaliverkko) ja auki piirrettynä. Olen yhdistänyt kuvaan L2- ja L3-VPN- referenssimallit [Aug06][Cal05] ja näiden mukaisen verkon. Kuvan toiminteet ja rakennusosat on selitetty alla olevassa taulukossa 2.



Kuva 3. Leimakytkentäisten virtuaaliverkkopalveluiden toiminteet yleisellä tasolla

Taulukko 2. MPLS-VPN:ien toiminteet ja rakennusosat yleisellä tasolla

Asiakasyhteys, AC (*engl. Access Connection*): Asiakasyhteys on erillinen siirtoyhteys liityntäverkon läpi CE- ja PE-laitteiden välillä. Se voi olla erillinen fyysinen yhteys, looginen yhteys (esimerkiksi ATM VC tai Ethernet VLAN) tai IP-tunneli (toteutusvaihtoehtoina IPsec, L2TP tai MPLS)
Asiakaskohtainen virtuaaliverkkoinstanssi (kuvassa X): Kussakin PE-laitteessa on erillinen instanssi kutakin asiakasta ja palvelua kohden. Instanssilla huolehditaan virtuaaliverkkojen tietojen ja kytkentöjen erillisyydestä PE-laitteissa. Asiakasyhteys liitetään loogisesti tähän instanssiin. Riippuen virtuaaliverkkopalvelusta tällä instanssilla on eri nimityksiä, jotka on kerrottu palvelun yhteydessä.
Yleinen reititys- ja kytkentätoiminne (kuvassa Y): Kussakin PE-laitteessa voidaan ajatella olevan yleinen kytkentä- ja reititystoiminne, joka tekee normaaleja leimareitittimen toimintoja. Se tarjoaa VPN-palveluille lisäksi kaksi asiaa: kuljetustunnelit ja VPN:iin liittyvän signaloinnin muihin PE-laitteisiin.

Kuljetustunnelit: Kuljetustunneli on tunneli läpi runkoverkon, jota PE-laitteiden välinen liikenne käyttää. Mikäli runkoverkko on leimakytketty, on kuljetustunneli yleensä leimakytketty polku. Eri virtuaaliverkkoyhteydet voivat käyttää samaa kuljetustunnelia, jolloin samojen PE-laitteiden väliset VPN-tunnelit laitetaan samaan kuljetustunneliin. Tässä hyödynnetään hierarkkista leimakytkentää. Kuljetustunnelit eivät ole yleisesti käytetty nimitys, mutta tämän työn kannalta tärkeänä käsitteenä olen katsonut parhaaksi antaa niille erillisen nimityksen. Kuljetustunneleista tarkemmin alaluvussa 2.4.2.
VPN-tunneli (*engl. VPN tunnel*): VPN-tunneli yhdistää eri PE-laitteissa olevat samaan virtuaaliverkkoon kuuluvat asiakaskohtaiset virtuaaliverkkoinstanssit toisiinsa. Eri virtuaaliverkkopalveluiden yhteydessä VPN-tunnelista voidaan käyttää hieman eri nimityksiä.
Merkinanto (*engl. signaling*): Virtuaaliverkkopalvelusta riippuen PE-laitteilla on erilaisia merkinantotarpeita keskenään. Eri virtuaaliverkkopalveluissa käytetään myös eri mekanismeja PE-laitteiden ja asiakaskohtaisten virtuaaliverkkoinstanssien väliseen tiedonvaihtoon. Signalointiin liittyen on lisäksi hyvä huomata, että jotta PE-laitteet voivat kommunikoida keskenään ja muodostaa kuljetustunnelin välilleen, on niiden huolehdittava normaalista IP:hen ja MPLS:ään liittyvästä signaloinnista runkoverkon laitteiden kanssa. Lisäksi on hyvä huomata, että tietyissä tapauksissa eri toimipisteissä olevilla laitteilla voi olla suora signalointiyhteys keskenään (ne voivat esimerkiksi olla reititysnaapureita), jolloin virtuaaliverkkopalvelu ei osallistu tähän signalointiin mitenkään: se on toimipisteiden välistä liikennettä siinä missä muukin liikenne.
Asiakashallintatoiminne (*engl. Customer management function*)(ei käsitellä tässä työssä): Voidaan mieltää osaksi runkoverkkoa. Se pitää sisällään asiakaskohtaiset tiedot, kuten yhteystiedot, tiedot asiakkaan liitännöistä, palvelun laadusta, rajoituksista, laskutuksesta ja muista vastaavista seikoista.
Verkonhallintatoiminne (*engl. Network management function*) (ei käsitellä tässä työssä): Verkonhallinta voidaan mieltää osaksi runkoverkkoa. Toiminteen avulla provisioidaan ja monitoroidaan verkon laitteita.

2.4.2 Reunareititinten väliset tunnelit, "kuljetustunnelit"

Leimakytketyssä verkossa muodostuu leimakytkettyjä polkuja leimareititinten välille. Liikenne, jonka on tarkoitus kulkea samaa reittiä verkossa, voi hyödyntää samaa leimakytkettyä polkua pakettien välitykseen. Tällaista leimapolkua kutsutaan tässä työssä kuljetustunneliksi silloin, kun VPN-liikenne hyödyntää sitä kahden virtuaaliverkkoinstanssin välillä. Leimoja, joiden avulla kuljetustunneli muodostuu,

kutsutaan tässä työssä *kuljetusleimoiksi*[17]. Vastaavaa tunneliyhteyttä kutsutaan kuljetustunneliksi, vaikka se olisi toteutettu muuten kuin leimakytkennän avulla. Kuljetustunnelista käytetään IETF-dokumentaatiossa usein termiä PSN tunnel (*engl. Packet Switched Network tunnel*). [Aug06][Cal05]

Leimakytkettyjen kuljetustunnelien käyttö PE-reititinten välillä edellyttää, että reitittimillä on leimat toistensa osoitteille, joissa verkko-osa on koko IP-osoitteen mittainen (IPv4:ää käytettäessä verkkomaski on 32 bittiä pitkä). Tämä edellyttää tarkan osoitteen mainostusta leimanjakelun lisäksi myös reitityksessä.

Useimmiten verkon läpi vievät leimakytketyt polut on signaloitu LDP-protokollalla automaattisesti IGP-protokollalta saadun reititystiedon ja verkkotopologian mukaisesti. Joissain verkoissa, joissa käytetään tiukempaa liikenteen hallintaa (TE), käytetään RSVP:tä vastaavien LSP:iden luomiseen. Joissain verkoissa käytetään sekä LDP:tä että RSVP:tä. [Dav00]

Jos halutaan muodostaa leimapolku kahden verkon välillä, ei voida hyödyntää IGP-protokollaa. Tällöin käytetään yleensä BGP-protokollaa sekä reititystiedon että leimojen välittämiseen.

Jotkut operaattorit eivät halua käyttää runkoverkossaan lainkaan leimakytkentää, mutta haluavat silti tarjota MPLS:ään perustuvia virtuaaliverkkopalveluita. Tällöin reunareititinten välisessä tunneloinnissa käytetään leimattujen pakettien pakkaamista IP-paketteihin PE-reitittimien välillä. Tällainen IP-tunnelointi voi perustua esimerkiksi GRE- tai IPsec-protokolliin. [Rek07][Ros05]

Virtuaaliverkkopalveluiden kannalta olennaisinta on, että on olemassa tunneli, jota pitkin VPN-leimatut virtuaaliverkon paketit pääsevät reunareitittimeltä toiselle. Tekniikka, jolla tämä toteutetaan, on toissijainen. Palvelun laadun ja verkon suorituskyvyn kannalta tunneloimistekniikalla saattaa olla merkitystä, mutta tätä vaikutusta ei tässä työssä analysoida. [Cal05] [Aug06]

2.4.3 Leimakytkentäisen virtuaaliverkkopalvelun hallintatason toiminta

Kaikilla tässä työssä esitellyillä virtuaaliverkkopalveluilla on samantapaiset hallintatason toiminnat. Se, miten nämä toiminnallisuudet on toteutettu kussakin virtuaaliverkkopalvelussa, on selitetty palvelukohtaisessa alaluvussa. Hallintatason toiminteet voidaan jakaa neljään kokonaisuuteen:

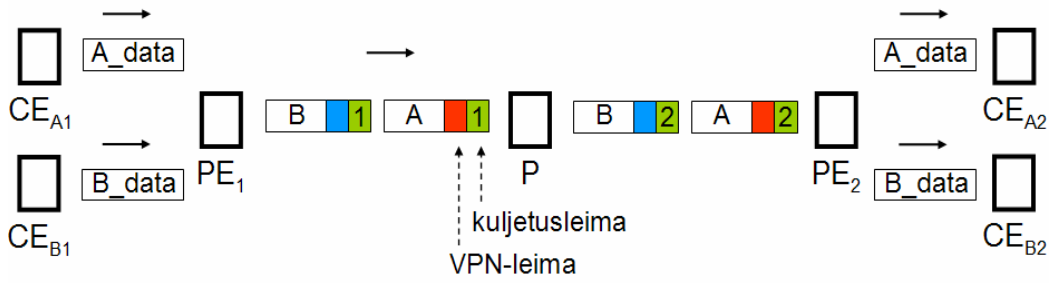
---

[17] Joissain yhteyksissä kuljetusleimasta käytetään nimitystä IGP-leima. Inter-AS:ssä kuljetusleima ei ole välttämättä sidottu yhteen IGP-alueeseen.

1. Muiden PE-reititinten löytäminen, joissa on tietyn virtuaaliverkon toimipisteitä kytkettynä.
2. Kuljetustunnelien luominen tai valitseminen, jolla PE reititin voi lähettää liikennettä niille PE-reitittimille joissa on tietyn virtuaaliverkon toimipisteitä kytkettynä.
3. VPN-leimojen signalointi, jonka avulla PE-reititin osaa lähettää kuljetustunnelista vastaanottamansa paketin oikean virtuaaliverkon oikeaan toimipisteeseen.
4. VPN-signalointi, jolla voidaan kertoa virtuaaliverkon sisäisestä topologiasta tai sen muutoksista.

2.4.4 Paketin kulku leimakytketyssä virtuaaliverkossa

Kuvassa 4 on esitetty kahteen eri virtuaaliverkkoon kuuluvien asiakkaiden VPN-paketin kulku leimakytketyn verkon läpi[18]. Asiakkaan A liikenne on matkalla asiakaslaitteelta CE_{A1} asiakaslaitteelle CE_{A2} ja asiakkaan B vastaavasti CE_{B1}:ltä CE_{B2}:lle. CE_{A1} ja CE_{B1} on kytketty samaan operaattorin PE-reitittimeen, kuten myös CE_{A2} ja CE_{B2}. Värikkäät neliöt pakettien edessä niiden matkatessa PE_1:ltä PE_2:lle kuvaavat MPLS-leimoja. Vihreät ovat kuljetusleimoja ja punaiset ja siniset VPN-leimoja.



Kuva 4. Virtuaaliverkkoon kuuluvan paketin kulku leimakytketyssä verkossa

Kuva 4 havainnollistaa seuraavia MPLS-VPN:ille olennaisia asioita:

- Ensimmäinen PE tekee VPN-paketin kytkentäpäätöksen ja tarvittavat toimenpiteet, jotta paketti pääsee oikealle yhteydelle kohden ulosmeno-PE:tä.
- Samojen PE-reititinten välisessä liikenteessä eri virtuaaliverkkoihin kuuluva liikenne voi jakaa saman kuljetustunnelin (huomaa kuljetusleimojen arvot).

[18] Kuvassa ei ole selkeyden vuoksi ennakoivaa leimanpoistoa (*engl. Penultimate hop popping*).

- P-reititin tekee kytkentäpäätöksen vain päällimmäisen leiman (kuljetusleima) perusteella, eikä koske alla oleviin leimoihin.

2.5 BGP-protokollaa ja leimakytkentää hyödyntävä IP-virtuaaliverkkopalvelu

BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot on esitelty alun perin IETF:n dokumentissa RFC 2547. Tässä työssä käsitellään palvelun uudistettua versiota, joka on julkaistu RFC:nä 4364. RFC 4364 tunnetaan myös nimellä "Rfc2547bis" työnimensä mukaisesti. Palvelun perustoteutus on sama molempien dokumenttien mukaan, uudistettu versio lähinnä tarkentaa alkuperäisessä dokumentissa avoimeksi jääneitä asioita.

2.5.1 Palvelun lyhyt kuvaus

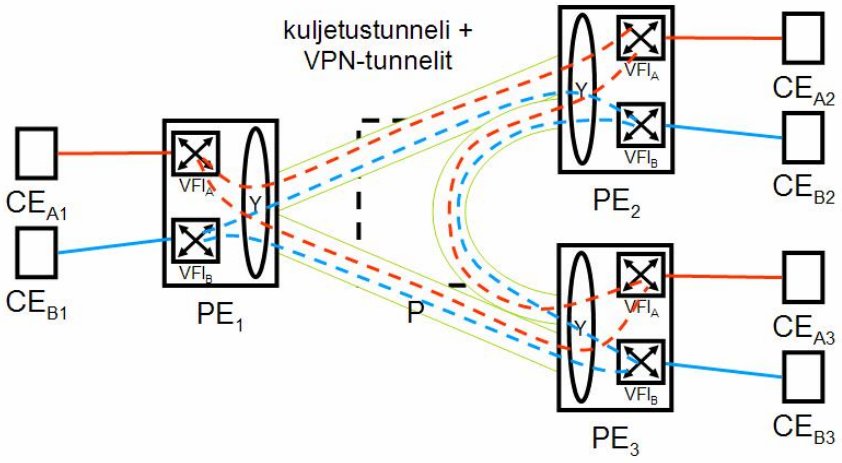
BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot -palvelu tarjoaa asiakkaalle IP-verkon toimipisteiden (CE-laitteiden) välille. Sitä sanotaan L3-virtuaaliverkoksi, koska IP:n katsotaan kuuluvan OSI-mallin verkkokerrokselle (Layer 3). Vaikka on olemassa muitakin ehdotuksia L3-virtuaaliverkkopalveluksi, tässä työssä L3-VPN viittaa tähän palveluun, ellei tosin mainita. Toimipisteiden lukumäärää ei ole rajattu. Palvelu takaa osaltaan, että asiakkaan verkko on sekä riippumaton muiden verkkojen osoitteistuksesta ja reitityksestä että eristetty muusta verkosta (suljettu käyttäjäryhmä, turvattu liikennöinti). Palvelussa operaattori(t) huolehtii runkoverkon toiminnan lisäksi liikenteen ja reititysinformaation kulusta toimipisteiden välillä eli ns. *VPN-reitityksestä*. [Ros06a]

2.5.1.1 Palvelun erikoistapaus: leimakytkentäinen asiakas (Carriers' Carrier)

RFC:ssä 4364 on määritelty erikoistapaus operaattori-VPN (*engl. Carriers' Carrier*, CsC), jossa asiakasliikenne on leimakytkettyä IP-liikenteen sijaan. Tällöin VPN-operaattorin ei tarvitse huolehtia varsinaisesta asiakasreitityksestä, vaan ainoastaan signaloida leimat, joilla asiakastoimipisteiden reitittimet osaavat lähettää liikennettä toisilleen. Varsinainen reititys tapahtuu asiakkaan CE-laitteiden välillä, eikä näy runkoverkon operaattorille lainkaan. Käytännössä tämä lisää leimapinoon ylimääräisen leiman, jolla varmistetaan, että asiakkaalta tuleva leimattu liikenne ei voi suuntautua minnekään muualle kuin saman asiakkaan toimipisteisiin. [Ros06a]

2.5.2 L3-VPN:n referenssimalli ja rakennusosat

RFC4364-palvelun *referenssimalli* on kuvassa 5. Se noudattaa yleistä referenssimallia sillä täsmennyksellä, että asiakaskohtainen virtuaaliverkkoinstanssi on L3-VPN:ssä virtuaaliverkon välitysinstanssi (*engl. VPN Forwarding Instance*, VFI) [Cal05]. Referenssimallissa olevien laitteiden lisäksi L3-VPN-palvelun toteuttamisessa käytetään usein reittiheijastinta (*engl. Route Reflector*, RR), vaikka se ei varsinaiseen referenssimalliin kuulukaan. RFC4364-palvelun toiminteet, joita ei esitelty MPLS-VPN:ien yhteisten komponenttien yhteydessä alaluvussa 2.4, on koottu oheiseen taulukkoon 3.



Kuva 5. RFC:n 4364 mukaisen L3-VPN:n referenssimalli

Taulukko 3. RFC4364-spesifiset rakennusosat ja toiminteet

Virtuaaliverkon välittäjäinstanssi (*VPN Forwarding Instance*), **VFI**: VFI on VPN-kohtainen instanssi PE-reitittimessä. Jokaisessa PE:ssä on yhtä monta VFI:tä kuin siinä on eri L3-virtuaaliverkkoihin liitettyjä toimipisteitä kytkettynä. Kukin VFI sisältää VPN-kohtaisen kytkentä- ja reititystaulun (VRF-taulu, *engl. VPN Routing and Forwarding table*). Siksi VFI:stä käytetään usein termiä **VRF-toiminne** (tai lyhyemmin **VRF**)
Reittiheijastin (*Route Reflector*), **RR**: Reittiheijastin toimii PE-reitittimien välisen BGP-signaloinnin välityssolmuna. Vain VPN-reititystietoa välittävästä RR:stä käytetään joskus nimitystä **VPN-RR**. Verkkoa voi segmentoida VPN-RR:ien avulla erillisiksi VPN-palvelualueiksi, joiden VPN-signalointi on täysin erillistä. RR voi hoitaa myös signaloinnin sisällön suodattamista. Tietyissä VPN-verkkojen yhteenliittämistavoissa RR:llä on erityisrooli, tähän palataan luvussa 3.

2.5.3 Liikenteen välitys

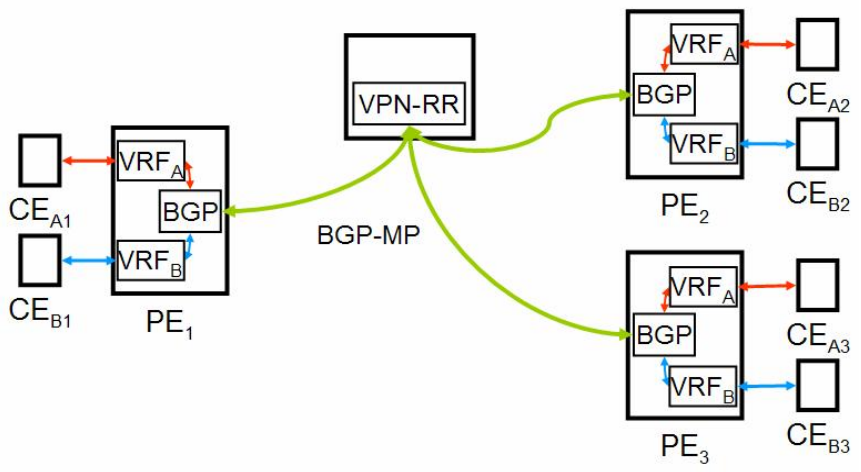
Liikenne yhdeltä virtuaaliverkkoon kuuluvalta toimipisteeltä toiselle kulkee L3-VPN:issä IP-paketteina CE-reititinten välillä. PE-reititinten välillä se kulkee leimattuna tai IP-tunneloituna. Alla on kuvattu paketin kulku. Tiedot, joilla kytkentäpäätökset tehdään, saadaan hallintatasolta, jota käsitellään alaluvussa 2.5.4.

Paketin kulku L3-VPN:ssä:

1. CEA1 lähettää IP-paketin asiakasyhteyden (AC) yli PE1:lle.
2. PE1 katsoo AC:n perusteella VFI:n, jonka VRF:n mukaan paketti kytketään (eli mihin VPN:ään toimipiste kuuluu).
3. PE1 katsoo VRF:stä, missä on IP-paketin otsakkeen ilmoittama kohdeosoite (eli mikä on next-hop kentän arvo reititystaulussa). Jos kohdeosoite on jonkin toisen PE:n takana (kuten kuvassa (Kuva 4) PE2:n takana), laittaa PE1 paketin eteen VPN-leiman (kuvassa punainen ja sininen leima) ja etsii paketille oikean "kuljetustunnelin" läpi runkoverkon.
4. Oikea "kuljetustunneli" löydetään next-hop -kentän perusteella.
    a. Leimakytkentää käytettäessä paketin päälle laitetaan toinen leima (ns. kuljetusleima, kuvassa vihreä leima), jonka avulla runkoverkko osaa ohjata paketin PE:hen (kuvassa PE2), joka on next-hop:ina kyseiselle reitille. Paketti lähetetään leimoilla varustettuna runkoverkkoon.
    b. Käytettäessä IP-tunnelointia, VPN-leimalla varustettu leima laitetaan siihen tunneliin, joka vie PE:hen, joka on next-hop:ina kyseiselle reitille.
5. Runkoverkon läpi paketti menee kuin mikä tahansa leimattu paketti, sillä VPN-leima ei näy runkoverkon P-reitittimille.
6. Ulostulo-PE osaa kytkeä paketin VPN-leiman perusteella oikealle ulosmeno-AC:lle kohti CE2:tä.

2.5.4 Hallintataso

BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot -palvelu hyödyntää BGP-protokollaa hallintatasollaan runkoverkon sisällä (eli PE-reititinten välillä). Asiakasyhteyksillä (CE-PE) voidaan käyttää jotakin reititysprotokollaa, kuten BGP:tä tai OSPF:ää, tai staattista reititystä. Kuva 6 esittelee "VPN-reititysketjun" eli komponentit, jotka käsittelevät VPN-reittien välityksessä käytettäviä reitityssanomia. [Ros06a]



Kuva 6. RFC:n 4364 mukaisen L3-VPN-signalointi

2.5.4.1 BGP-protokollan käytöstä

BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot käyttävät BGP:tä neljään eri tarkoitukseen: PE-reititinten löytämiseen, PE:n osoitteen mainostamiseen reititystä varten, VPN-leimojen signalointiin ja VPN-kohtaisen reititystiedon välitykseen. Nämä asiat tapahtuvan samanaikaisesti ja samalla BGP-mekanismilla.

Voidakseen hyödyntää BGP:tä, tulee PE-reitittimillä olla tietojen välittämiseen kykenevä BGP-yhteys keskenään. L3-VPN-reitityksessä hyödynnetään BGP:n moniprotokollalaajennusta (BGP-MP) [Bat07]. BGP-MP:n avulla L3-VPN-osoitteet voidaan mainostaa omana osoiteperheenään VPNv4 (*engl. VPN-IPv4 address family*) käyttäen omaa saavutettavuusryhmäänsä (*engl. Network Layer Reachability Information*, NLRI). Tällöin osoitteet pysyvät BGP-prosessissa erillään ”normaaleista” IPv4-unicast-osoitteista. VPNv4-osoitteet ovat IPv4-osoitteita, joihin on lisätty reittierotin (*engl. Route Distinguisher*, RD).

Reittierotin eli Route Distinguisher:

Jokaisella virtuaaliverkolla tulee olla eri reittierotin (RD). Sen avulla eri VPN:ien IP-osoitteistukset voivat mennä päällekkäin ilman vaaraa, että osoitteet sekoittuisivat reitityksessä.[Ros06a]

RD on suunniteltu niin, että kukin operaattori voi hallinnoida omaa "RD-numeroavaruuttaan". Operaattorin valinnan mukaan RD sisältää joko IP-osoitteen tai AS-numeron ja tämän lisäksi juoksevan numeron. Operaattori voi käyttää RD-arvoina esimerkiksi omaa AS-numeroaan ja tämän perässä asiakaskohtaista juoksevaa numeroa. Toinen selkeä vaihtoehto on käyttää PE-reittimen IP-osoitetta ja asiakasnumeroa. AS-numeron käyttöä puoltaa yksinkertaisuus ja se, että näin jää enemmän tilaa asiakasnumeroinnille (32 bittiä 16 sijaan). IP-osoitteen käyttöä puoltaa reittien alkuperän selkeys. Lisäksi se voi auttaa tietyissä liikenteen hallintaan liittyvissä tilanteissa. Kummatkin tavat hajauttavat RD-arvojen hallinnoinnin operaattoreille varmistaen samalla globaalisti yksilölliset VPN-IPv4-osoitteet . [Ros06a]

PE-reititin lisää RD-arvon siinä vaiheessa, kun asiakkaalta mainostuva IPv4-reitti viedään PE:n BGP-tauluun ja siitä tehdään VPNv4-reitti. Se määritellään siis jokaisessa PE:ssä erikseen kullekin VPN:lle. [Ros06a]

PE:t voivat olla joko BGP-naapureita, taikka ne voivat olla yhdistettyinä yhteisen reittiheijastimen (RR) välityksellä. RFC4364-palvelu käyttää BGP:n standardia moniprotokollalaajennusta (BGP-MP) ja VPNv4-osoiteperhettä eikä muuta BGP:n mekanismeja mitenkään. Kaikki yleiset BGP:n toiminnallisuudet pätevät siihen. [Ros06a]

Seuraavissa alaluvuissa on käsitelty sitä, miten RFC4364-palvelussa toteutetaan alaluvussa 2.4.3 mainitut neljä toiminnetta.

2.5.4.2 PE-reititinten löytäminen L3-VPN-palvelussa

BGP-reititys on ”yksisuuntaista”. Kukin BGP-puhuja mainostaa reittejään BGP-naapureilleen, mutta reittimainostuksen vastaanottavan naapurin tehtäväksi jää punnita mainostusten arvo. Kunkin reitin kohdalla naapuri voi punnita itse lisätäkö reitti reititystauluun vai hylätäkö se; lisätessään se voi itsenäisesti päättää minkälaisia määritteitä se liittää saamiinsa reititystietoihin[19]. Reititystiedon lähettäjälle ei

[19] Tämä päättely perustuu toisaalta normaaliin BGP-prosessiin, toisaalta reitittimen konfiguraatioihin, jotka puolestaan on johdettu operaattorin reitityspolitiikasta.

raportoida tiedon käytöstä, mistä johtuen reititysinformaation lähettäjällä ei ole suoraa tietoa, millä tavoin vastaanottaja käyttää saamaansa reititysinformaatiota[20].

RFC4364:n mukaisissa VPN:ssä BGP:n yksisuuntaisuutta hyödynnetään seuraavasti: Kaikki VPN-informaatio (eli reittimainostukset) välitetään kaikille L3-VPN-BGP-naapureille ja annetaan vastaanottavien PE-reititinten selvittää, onko niillä mainostettuun virtuaaliverkkoon kuuluvia toimipisteitä kytkettyinä. Tämä päättely tehdään VPNv4-reittien mukana kulkevien kohdesuotimen (*engl. Route Target*) arvojen avulla.

Kohdesuodin eli Route Target –attribuutti:

Kohdesuodin (RT) on BGP:n attribuutti. Se on määritelty RFC:nä 4360 *"BGP Extended Communities Attribute"* [San06]. RFC määrittelee RT:n muodon, sen käyttö on määritelty L3-VPN:n palvelukuvauksessa [Ros06a].

Rakenteeltaan kohdesuodin on samanlainen kuin reittierotin (RD). Se koostuu kahdesta osasta. Ensimmäisessä osassa operaattori voi käyttää joko AS-numeroa tai IP-osoitetta. Loppuosa RT:stä jää operaattorin vapaasti valitsemalle tunnistenumerolle. Usein operaattorit jakavat tämän osan vielä kahtia: asiakaskohtaiseen ja VPN-topologiasta kertovaan osaan.

RT on VPN-reittimainostuksen virtuaalinen "klubikortti". Tiettyyn VPN:ään kuuluvalla reitillä on tietyn "värinen" (numeroarvoinen) kortti (RT). Reitin kuuluminen eri "klubeihin" määrittyy sen mukaan, minkä VFI:n kautta reitti runkoverkkoon tulee. Reitti saa yhden tai useamman RT:n sen mukaan, mitä Export Target -arvoja kyseiseen VFI:hin on konfiguroitu.

Reitin pääseminen muihin VFI:en reititystauluihin riippuu siitä, vastaako reitin mukana oleva RT-arvo vastaanottavaan VFI:hin konfiguroitua Import Target -arvoa. Jos reitillä on monta Export Target -arvoa, riittää, että joku reitin RT-arvoista vastaa (jotain) VFI:n Import Target -arvoa, jolloin reitti lisätään VRF-tauluun.

Yksinkertaisimmillaan kaikilla samaan virtuaaliverkkoon kuuluvilla toimipisteillä (tai oikeammin VFI:llä, joihin toimipisteet kytketään) on samat Export- ja Import Targetit. Tällöin muodostuu VPN, joka on topologialtaan täysin kytketty (*engl. full-mesh*). Haluttaessa muunlaisia VPN-topologioita määritellään samaan virtuaaliverkkoon kuuluviin VFI:in epäsymmetritset Export- ja Import Targetit.

[20]Jos BGP-naapurit ovat myös pakettien välitystasolla naapurit, voi BGP-puhuja päätellä reititystiedon käytöstä epäsuorasti tarkkailemalla ko. naapurilta tulevaa liikennettä. Jos naapuri välittää ko. reittimainostuksen reitteihin menevää liikennettä reitin mainostajan kautta, on reititystieto käytössä (jos liikennettä ei ole, se ei vielä välttämättä kerro siitä, onko reitti päätynyt reititystauluun).

PE-reititin ”löytää” muut PE:t, joilla on saman VPN:n toimipisteitä, tarkkailemalla BGP-MP-sanomia. Jos sanomassa on sama RT-arvo, joka löytyy jostain PE:n VFI:stä import targetina, on reittimainostuksen alullepanijalla yhteisiä VPN:iä PE:n kanssa. Tämä alullepanijan[21] osoite (=identiteetti) löytyy BGP:n VPNv4-reittimainostuksessa NEXT_HOP-attribuutista (NH). [Ros06a]

RFC4364:n on julkaistu laajennus ”*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*” [Mar06b], jota käyttämällä kaikkia BGP:n välittämiä reittejä ei tarvitse mainostaa kaikille PE-reitittimille. Tässä toimintamallissa PE voi mainostaa import target –arvonsa muille, jolloin reittikeskitin voi suodattaa reitit, jotka eivät sisällä näitä vastaavia RT-arvoja, pois tälle PE:lle menevistä reittimainostuksista. [Mar06b]

Edellä olevasta seuraa, että verkossa tieto VPN:ien koostumuksesta on hajallaan PE-reitittimissä, mutta ei (välttämättä) keskitetysti missään. Jos käytetään erillistä provisiontijärjestelmää, sillä on luonnollisesti tieto luomistaan virtuaaliverkoista. Lisäksi, jos verkossa ei erityisesti suodateta BGP-sanomia, kuten oletusarvoisesti ei tehdä, on kaikkien verkon VPN:ien tiedot mahdollista kerätä liittymällä RR:n BGP-asiakkaaksi ja keräämällä kaikki saapuvat BGP-sanomat.

2.5.4.3 Kuljetustunnelien valitseminen L3-VPN-palvelussa

Kuljetustunneli valitaan BGP:n VPNv4-reittimainostuksessa reittiä vastaavan NH-kentän arvon perusteella. Leimakytkentäisessä verkossa tälle arvolle pitäisi löytyä kuljetusleima ja IP-tunnelointia hyödyntävässä tunneliliitäntä.

2.5.4.4 VPN-leimojen signalointi L3-VPN-palvelussa

VPN-leimat, joiden avulla PE:t osaavat kytkeä runkoverkosta tulevan VPN-liikenteen, signaloidaan BGP:n VPNv4 reittimainostuksissa osana NLRI-informaatiota (*engl. Network Layer Reachability Information*). [Rek01]

2.5.4.5 VPN-reititys L3-VPN-palvelussa

L3-VPN-palvelussa asiakasreitin CE voi vaihtaa saavutettavuustietoja PE-reitittimen kanssa jollain dynaamisella reititysprotokollalla tai saavutettavuustiedot voidaan konfiguroida VFI:hin (staattinen reititys). Kun näitä tietoja vaihdetaan eri toimipisteiden välillä, käytetään nimitystä VPN-reititys. RFC4364:ssä tämä hoidetaan BGP:n VPNv4 reittimainostuksissa osana NLRI-informaatiota. [Ros06a]

---

[21] Inter-AS:n tapauksessa NH ei välttämättä kerro reitin alullepanija PE:tä, vaan se saattaa kertoa AS-alueen rajareitittimen, ASBR:n.

2.5.5 Yhteenveto RFC 4364:n mukaisesta virtuaaliverkkopalvelusta

Jatkotyön kannalta olennaisimmat BGP-protokollaa ja leimakytkentää hyödyntävän IP-virtuaaliverkkopalvelun ominaisuudet ja toiminnot ovat:

- BGP-protokollaa ja leimakytkentää hyödyntävät IP-virtuaaliverkot -palvelulla operaattori tarjoaa asiakkaalle IP-protokollan mukaisen virtuaaliverkon. Asiakasliikenne välitetään VPN:n sisällä IP-osoitteen perusteella.
- RFC4364-palvelu olettaa, että PE-laitteiden välillä on kuljetustunnelit. Palvelu itse ei luo niitä.
- PE-reitittimien välillä kaikkeen VPN-palveluun liittyvään signalointiin käytetään BGP-protokollaa moniprotokollalaajennuksin. BGP-MP-yhteys voi olla joko suoraan kytketty tai siinä voidaan käyttää hyväksi BGP:n keskitystoiminnetta, reittiheijastinta.
- BGP-signaloinnin mukana kulkevien tietojen kulkua rajoittaa:
  1. Tietoa lähetetään vain konfiguroidulle BGP-naapurille.
     - Tämä naapuri edelleenlähettää tietoja erikoistapauksessa[22] omille naapureilleen.
  2. Tietoja lähetetään vain niille BGP-naapureille, joiden kanssa on konfiguroitu VPNv4-osoiteperhe käyttöön.
  3. Suodattaminen esimerkiksi RT-arvojen perusteella.
- Asiakasreittien lisäksi VPN-signaloinnissa välittyy PE-reitittimen oma osoite Next-Hop-attribuutissa tunnistetietoja, joissa mahdollisesti on tietoa PE-reitittimen osoitteesta.
- VPN-signaloinnissa on lisäksi tunnistetietoja, joissa voi olla PE-reitittimen osoitetietoja riippuen operaattorista. Näitä tietoja ovat:
  1. Reittierotin (Route Distinguisher)
  2. Route Target
  3. Site Of Origin[23] (ei käsitelty edellä: omaa saman rakenteen kuin RD ja RT).
- RT-arvoja käytetään yhdessä PE-reititinten tuonti- ja vientikäytäntöjen kanssa rajoittamaan VPN-reittien mainostumista. Tätä hyödynnetään virtuaaliverkkojen automaattisessa muodostamisessa.

---

[22] Reittiheijastin on tyypillisin tällainen erikoistapaus. Toinen on ASBR, joka on erikseen konfiguroitu lähettämään reititystietoja toiseen AS:ään.

[23] SoO:ta käytetään ehkäisemään reititysluuppien muodostuminen tietyissä verkkorakenteissa (lähinnä multihoming).

2.6 Virtuaalijohdinpalvelu

IETF:n L2vpn-työryhmä ei ole julkaissut *Virtuaalijohdinpalvelun* (VPWS, *engl. Virtual Private Wire Service*) toteutusta kuvaavaa dokumenttia. Tästä on haittaa enemmän tälle työlle kuin Virtuaalijohdinpalvelun käytännön toteutukselle[24]. Tässä alaluvussa esitelty palvelu on ennemmin kokoelma standardoituja tekniikoita kuin standardoitu palvelu.

L2-virtuaaliverkkojen kehysdokumentissa *"Framework for Layer 2 Virtual Private Networks (L2VPNs)*" (RFC 4664) on kuitenkin kuvattuna muiden L2-VPN:ien ohella myös VPWS-palvelun referenssimalli ja toiminnalliset osat. Palvelun ydin – virtuaalijohtimet ja niiden signalointi – on määritelty IETF:n Pwe3-työryhmän toimesta. Koska L2-tekniikoita on useita, on määrittelydokumenttejakin useita. Keskeisin niistä on *"Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*" (RFC 4447). Tämän lisäksi IETF:ssä on työn alla monesta pätkästä koostuvat virtuaalijohtimet, niitä käsitellään inter-AS-tarkastelun yhteydessä luvussa 3.

2.6.1 Palvelun lyhyt kuvaus

Virtuaalijohdinpalvelussa operaattori tarjoaa asiakkaalle kahden reunalaitteen (CE:n) välille siirtoyhteyden niin, että ne näyttävät olevan liitetty yhteen loogisella L2-piirillä. Yhteys kuljettaa kaikki CE:ltä PE:lle lähetetyt L2-PDU:t (eli "L2-kehykset") sellaisenaan[25] palveluun liitetylle vastapään CE:lle. Paketin otsakkeen tiedot vaikuttavat vain liitäntäpiirin tunnistamiseen, eivät paketin kytkentään virtuaaliverkon sisällä. Virtuaalijohdinpalvelu käyttää toteutuksessaan virtuaalijohdinta (PW) kahden PE-laitteen välillä. [Aug06]

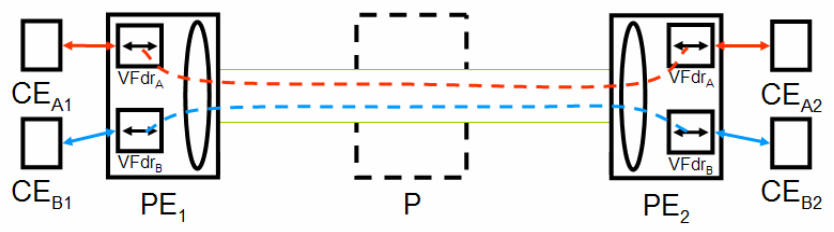
---

[24] Operaattori voi palvelua tuotteistaessaan päättää mitä olemassa olevista tekniikoista sen toteuttamiseen käytetään välittämättä onko palvelu "standardinmukainen" vai ei.

[25] Operaattori voi – asiakkaan kanssa sovitusta palvelusta – riippuen tehdä L2-PDU:iden otsakkeille tiettyjä asioita, esimerkiksi muuttaa osoitetta tai lisätä tai poistaa VLAN-otsakkeita, erikoistapauksessa jopa tehdä muunnoksen L2-tekniikasta toiseen.

2.6.2 Virtuaalijohdinpalvelun referenssimalli ja rakennusosat

Virtuaalijohdinpalvelun referenssimalli on esitetty kuvassa 7. Kuvassa on kaksi eri virtuaalijohdinyhteyttä (CE_{A1}-CE_{A2} ja CE_{B1}-CE_{B2}). Alla olevassa taulukossa 4 ovat yleisestä referenssimallista poikkeavat rakennusosat selityksineen. [Aug06]



Kuva 7. Virtuaalijohdinpalvelun referenssimalli

Taulukko 4. VPWS-referenssimallin mukaiset rakennusosat:

Toistaja (*engl. Forwarder*), VFdr[26]: Virtuaaliverkkokohtainen instanssi PE-reitittimessä, joka vastaanottaa siirtoyhteyskerroksen datapaketit ja ”toistaa” ne edelleen virtuaalijohtimelle.
Virtuaalijohdin (engl. *pseudowire*): PE-laitteiden välinen yhteys, jota pitkin VFdr:t pystyvät lähettämään VPN-datapaketteja. Näistä käytetään myös nimitystä emuloidut piirit. Virtuaalijohdin vastaa yleisen mallin VPN-tunnelia.

2.6.3 Liikenteen välitys

Liikenne yhdeltä virtuaaliverkkoon kuuluvalta toimipisteeltä toiselle kulkee virtuaalijohdinpalvelussa siirtoyhteysprotokollan mukaisina L2-PDU:ina – paketteina, soluina tai kehyksinä – CE-laitteiden välillä. PE-reititinten välillä se kulkee virtuaalijohtimessa leimattuna tai IP-tunneloituna. Liikenteen välitys sinänsä on hyvin yksinkertaista: jokainen PE:lle liitäntäpiiriltä tuleva paketti välitetään virtuaalijohdinta pitkin toiselle PE:lle ja siellä edelleen liitäntäpiirille. [Aug06]

Virtuaalijohdinpalvelun tekniikkakirjoa rajoittavat käytännössä PE-laitteen liitännät ja toisaalta enkapsulointimäärittelyt. Enkapsulointeja on määritelty seuraaville L2-tekniikoille: TDM [Rie05][Vai06], Ethernet [Mar06c], Frame Relay [Mar06d], PPP [Mar06e], HDLC [Mar06e], ATM [Mar06f][Mal07] ja SDH [Mal07b]. Koska runkoverkon kannalta emuloitavalla tekniikalla ei ole merkitystä, enkapsulointimekanismeja ei käydä tässä työssä läpi.

[26] Toistajalle ei ole yleisesti käytettyä lyhennettä. VFdr-lyhennettä käytetään vain tässä kuvassa.

2.6.4 Hallintataso

Koska virtuaalijohdinpalvelua ei ole standardoitu, sen hallintataso ei ole kovin selkeä. Eri toiminnallisuudet voidaan toteuttaa eri protokollilla ja samakin toiminnallisuus voidaan toteuttaa useammalla eri tavalla ja protokollalla [Aug06]. Tähän lukuun olen valinnut toteutustavan, joka vastaa käsitystäni yleisimmästä toteutustavasta sekä eri valmistajien että operaattorien keskuudessa.

2.6.4.1 PE-reititinten löytäminen

Virtuaalijohtimien provisiontimalli määrittelee PE-reititinten löytämisen VPWS-palvelussa. RFC 4664 määrittelee kolme erilaista virtuaalijohtimien provisiointimallia: kaksisuuntaisen (*engl. Two-sided provisioning*), yksisuuntaisen (*engl. Single-sided provisioning*) ja niin sanottuihin väritettyihin ryhmiin (*engl. colored pools*) perustuvan.

Yleisimmin käytössä olevassa, kaksisuuntaisessa virtuaalijohtimien provisiointimallissa, PE-laitteisiin konfiguroidaan vastapään PE-reitittimen osoite [Aug06]. Tämä eliminoi PE-reititinten löytämisen tarpeen.

Yksisuuntaisessa provisoinnissa virtuaalijohdinyhteyden vastapää ilmaistaan ”globaalisti yksilöllisellä tunnisteella”. Tätä tunnistetta voidaan sitten hyödyntää PE-reititinten automaattiseen löytämiseen (*engl. auto-discovery*) [Aug06]. Yksisuuntainen provisionti on käytännössä sidottu LDP:hen, sillä siinä hyödynnetään LDP-protokollan laajennusta ”*Generalized ID FEC Element*”. Elementin kenttien käyttöä ei ole määritelty muuten kuin mainitsemalla, että niiden on oltava yksilöllisiä tietyllä VPN-palvelualueella [Mar06a]. Näin ollen yksisuuntaisen provisiointimallin avulla valitaan oikea PE-reititin PE-reitittimistä, joihin on jo LDP-signalointiyhteys.

Väritettyjä ryhmiä on ajateltu käytettäväksi lähinnä BGP-protokollan avulla soveltamalla moniprotokollalaajennusta (BGP-MP) ja siinä erillistä L2-osoiteperhettä. Tässä PE-reititinten ja toistimien löytäminen perustuu reittierottimien (RD) ja kohdesuotimen (RT) käyttöön samoin kuin RFC4364:n mukaisissa L3VPN:issä. RD:n ja RT:n lisäksi tarvitaan erillistä VPN-tunnusta. RD ja RT ovat operaattorin valittavassa samoin perustein kuin RFC4364-palvelussa. [Ros06b]

2.6.4.2 Kuljetustunnelin valitseminen

Kuljetustunneli valitaan kohde-PE:n IP-osoitteen perusteella. Tämä osoite on saatu selville jollain edellisessä alaluvussa esitellyistä PE-reitittimen löytämistavoista. Leimakytkentäisessä verkossa tälle osoitteelle pitäisi löytyä kuljetusleima ja IP-tunnelointia hyödyntävässä verkossa vastaavasti tunneliliitäntä.

2.6.4.3 VPN-leimojen signalointi

Virtuaalijohtimien VPN-leimojen signalointi tehdään joko LDP-protokollalla tai staattisesti konfiguroimalla. LDP-signalointi edellyttää suoraa yhteyttä PE-reititinten välillä. LDP:lle ei ole määritelty BGP:n kaltaista reittiheijastinta. PE:t voivat käyttää samaa LDP-yhteyttä kaikkien LDP:tä käyttävien VPN:ien signalointiin.[Mar06a]

Virtuaalijohtimia voidaan signaloida LDP:ssä kahdella eri tavalla. Ne eroavat käytetyn FEC-elementin mukaan: toinen käyttää yksinkertaisempaa ”*PWid FEC Element*” -tyyppiä (0x80) ja toinen monikäyttöisempää ”Generalized PWid FEC Element” -tyyppiä (0x81). Yksinkertaisempi FEC käy vain staattisesti konfiguroituihin virtuaalijohtimiin. Jos haluttaan käyttää PE:n automaattista löytämistä, on käytettävä monimutkaisempaa FEC-elementtiä. [Mar06a]

2.6.4.4 VPN-signalointi

Virtuaalijohdinpalvelussa ei signaloida mitään virtuaaliverkon sisäisiä osoitetietoja. Ainoa signaloitava asia on tilatieto siitä, että liitäntäpiiri on poikki. Tämä tehdään LDP-signaloinnissa poistamalla kyseinen VPN-leima. Varsinaiseen emuloitavaan L2-palveluun liittyvä signalointi tapahtuu itse hyötydatan joukossa (esimerkiksi OEM PDU:ina). [Mar06a]

2.6.5 Yhteenveto virtuaalijohdinpalvelusta

Jatkotyön kannalta olennaisimmat virtuaalijohdinpalvelun ominaisuudet ja toiminnot ovat:

- Virtuaalijohdinpalvelu tarjoaa asiakkaalle pisteestä-pisteeseen-yhteyden siirtoyhteyskerroksella.
- Palvelu olettaa, että PE-laitteiden välillä on kuljetustunnelit. Palvelu itse ei luo niitä.
- Virtuaalijohtimien luontiin PE-reitittimien välille käytetään niiden välistä suoraa LDP-yhteyttä. LDP-protokollaan on tehty laajennuksia L2-VPN-palveluita varten.
- PE-reititinten löytäminen on erotettu VPWS:ssä virtuaalijohtimien signaloinnista. Siihen voidaan käyttää esimerkiksi BGP-protokollaa.
- VPN-signaloinnissa ei kulje mitään asiakaan verkon tai identiteetin paljastavia tietoja[27].
- Jos BGP:tä käytetään PE-reititinten löytämiseen, siihen pätee samat seikat kuin L3-VPN:n kohdalla (tunnistetiedot, tietojen leviäminen ja sen rajoittaminen).
- Jos PE-reititinten automaattista löytämistä ei käytetä, lähetetään VPN-signalointia vain sille PE:lle, joka on kunfiguroitu kyseisen reitittimen vastapääksi.

---

[27] Toistimen identifioimiseen käytettävää numeroa ei tässä pidetä asiakastietona.

2.7 Virtuaalinen lähiverkkopalvelu

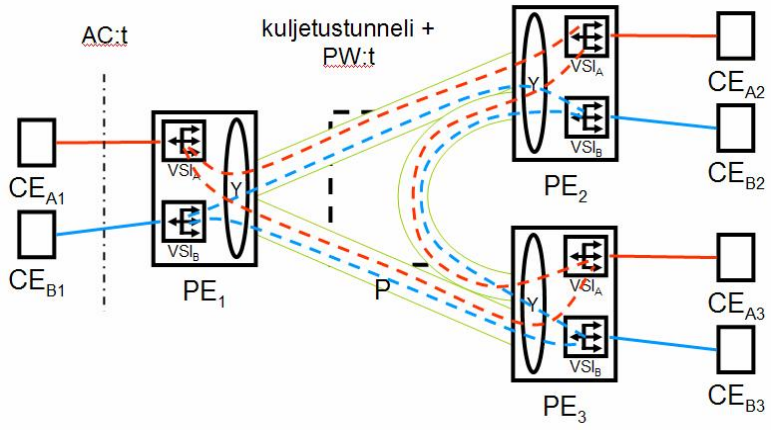
Virtuaalisen lähiverkkopalvelun (VPLS, *engl. Virtual Private LAN Service*) kohdalla IETF on tehnyt poikkeuksellisesti: se on julkaissut kaksi kilpailevaa toteutusehdotusta. Näistä RFC:nä 4762 julkaistu ”*Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*” on saanut laajemman laitevalmistajien tuen. RFC:nä 4761 julkaistun ”*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*” kohtalona on ollut jäädä lähinnä vain kehittäjänsä – Juniper Networksin – tukemaksi. Ratkaisuiden suurin tekninen ero on käytetty signalointiprotokolla, RFC 4762:ssa se on LDP, RFC 4761:ssä BGP. Ratkaisujen kattavuudessa on myös jonkin verran eroa, BGP-ratkaisun ollessa kattavampi. Koska tämän työn painopiste on yhteistoiminnassa, on esittelyn painopiste LDP-toteutuksessa, mutta esittelen samalla myös BGP-toteuksen.

2.7.1 Palvelun lyhyt kuvaus

Virtuaalisessa lähiverkkopalvelussa (VPLS) operaattori tarjoaa asiakkaalle virtuaalisen Ethernet-lähiverkon, johon voidaan liittää useita toimipisteitä. Asiakkaan CE-laitteille runkoverkko näyttäytyy yhtenä Ethernet-kytkimenä. VPLS hyödyntää virtuaalijohtimia (PW) PE-laitteiden välillä. VPLS:n voikin nähdä alaluvussa 2.6 esitellyn VPWS:n monipisteyhteysvastikkeena, johon on lisätty hieman kytkentä-älykkyyttä. [Aug06]

2.7.2 Virtuaalisen lähiverkkopalvelun referenssimalli ja rakennusosat

VPLS-palvelun referenssimalli on kuvassa 8. Se noudattaa yleistä referenssimallia sillä täsmennyksellä, että asiakaskohtainen virtuaaliverkkoinstanssi on VPLS:ssä virtuaaliverkon kytkininstanssi (VSI, *engl. Virtual Switch Instance*) [And05]. VPLS-palvelun toiminteet, joita ei esitelty MPLS-VPN:ien yhteisten komponenttien yhteydessä alaluvussa 2.4, on koottu oheiseen taulukkoon 5.



Kuva 8. Virtuaalisen lähiverkkopalvelun referenssimalli

Taulukko 5. VPLS:n rakennusosat

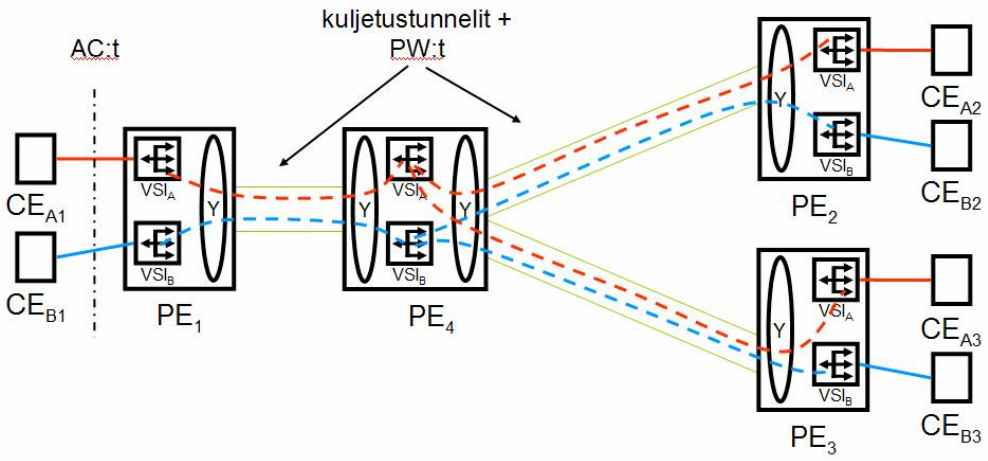
Virtuaaliverkon kytkininstanssi (*Virtual Switch Instance*), **VSI**: VSI on VPLS-kohtainen instanssi PE-reitittimessä. Jokaisessa PE:ssä on yhtä monta VSI:tä kuin siinä on eri VPLS-virtuaaliverkkoihin liitettyjä toimipisteitä kytkettynä. VSI suorittaa normaaleja Ethernet-kytkimen toimintoja. Pakettien välityksessä VSI voi hyödyntää sekä VLAN- että MAC-osoitetietoja.
Virtuaalijohdin (engl. *pseudowire*): PE-laitteiden välinen yhteys, jota pitkin VSI:t pystyvät lähettämään VPN-datapaketteja toisilleen. VPLS hyödyntää samoja virtuaalijohtimia kuin VPWS. Virtuaalijohdin vastaa yleisen mallin VPN-tunnelia.

Yhdessä VPLS:ssä kaikki VSI:t ovat kytkettyinä toisiinsa virtuaalijohtimilla. Poikkeuksen tähän tekee hierarkkinen VPLS (H-VPLS).

2.7.2.1 Hierarkkinen VPLS (H-VPLS)

RFC 4762 määrittelee VPLS:lle myös hierarkkisen toteutustavan. Toteutustavan ideana on vähentää sekä PE-reititinten välisten signalointiyhteyksien että virtuaalijohtimien tarvetta. RFC 4761:ssä ei ole määritelty hierarkkista toteutusta, sillä siinä voidaan vähentää signalointia BGP:n reittiheijastinta käyttämällä.[Las07][Kom07]

Kuvassa 9 on kuvattuna eräs H-VPLS-topologia. Huomattavaa on, että reitittimillä PE_1, PE_2 ja PE_3 ei ole kuljetutunnelia ja virtuaalijohtimia kuin PE_4:ään, jonka kautta ne kaikki ovat yhteydessä toisiinsa. H-VPLS ei näy muille PE-reitittimille; se on paikallinen konfiguraatio. H-VPLS-hierarkiatasojen määrää tai topologiaa ei ole rajoitettu. [Las07]



Kuva 9. Esimerkki hierarkkisesta VPLS:stä

H-VPLS vaikuttaa jonkin verran pakettien välityssääntöihin, tätä varten H-VPLS-PE:n tulee lajitella virtuaalijohdinyhteytensä keskus-PW:ihin (*engl. hub PW*) ja pinna-PW:ihin (*spoke PW*). [Las07] Tähän eroon palataan liikenteen välityksen yhteydessä.

2.7.3 Liikenteen välitys

Molemmissa palvelutoteutuksissa liikenteen välitys tapahtuu samalla tavalla. Liikenne kulkee Ethernet-kehyksinä toimipisteiden välillä. Kehykset voivat olla haluttaessa VLAN-otsakkeella varustettuja. PE-reititinten välillä liikenne kulkee virtuaalijohtimissa leimattuna tai IP-tunneloituna. Seuraavalla sivulla on kuvattu paketin kulku.

Paketin kulku VPLS-palvelussa:

1. CE_{A1} lähettää IP-paketin asiakasyhteyden (AC) yli PE_1:lle.
2. PE_1 katsoo AC:n perusteella VSI:n, jonka mukaan paketti kytketään (eli mihin VPN:ään toimipiste kuuluu).
3. PE_1 katsoo VSI:stä, onko sillä tietoa Ethernet-kehyksen lähde-MAC-osoitteesta[28] (minkä PW:n takana kohde on).
   - Jos ei, niin se lisätään kytkentätauluun yhdessä sen tiedon kanssa mistä liitännästä PDU tuli. Käynnistetään mahdollinen tiedon vanhenemisajastin.
   - Jos on, mutta paketti tuli eri liitännästä kuin kytkentätaulu ilmoittaa, taulukko päivitetään ja nollataan mahdollinen tiedon vanhenemisajastin.
   - Jos paketti tuli kytkentätaulun ilmoittamasta liitännästä, nollataan mahdollinen tiedon vanhenemisajastin.
4. PE_1 katsoo VSI:stä, onko sillä tietoa Ethernet-kehyksen kohde-MAC-osoitteesta.
   - Jos ei, niin paketti lähetetään kaikkiin muihin samaan VPLS-palveluun kuuluviin liitäntöihin paitsi siihen mitä se tuli.
     1. Jos paketti olisi tullut AC:n sijasta PW:ltä, niin se lähetettäisiin vain AC:ille, ei PW:ille.
     2. H-VPLS:ssä: Jos paketti olisi tullut AC:n sijasta keskus-PW:ltä, niin se lähetettäisiin vain AC:ille ja pinna-PW:ille, ei keskus-PW:ille[29].
   - Jos on, niin paketti lähetään vain siihen liitäntään, jonka kytkentätaulukko ilmoittaa.
5. Oikea "kuljetustunneli" valitaan PW:n next-hop-tiedon perusteella. Miten tämä tieto on saatu, riippuu PW:n signalointimenetelmästä.
6. Runkoverkon läpi paketti menee kuin mikä tahansa leimattu paketti, sillä VPN-leima ei näy runkoverkon P-reitittimille.
7. Ulostulo-PE katsoo PW-leiman perusteella VSI:n, jonka mukaan paketti kytketään (eli mihin VPN:ään toimipiste kuuluu).
8. Ulostulo-PE toistaa omalta kohdaltaan vaiheet 2 ja 3.

---

[28] MAC-osoite tulkitaan VLAN-kontekstissa, jos kehyksessä on VLAN-otsake.

[29] Pinna-PW ja AC ovat H-VPLS:ssä paketin välityksen kannalta samanlaisia.

2.7.4 Hallintataso

Hallintatasolla kilpailevat VPLS-standardit poikkeavat toisistaan täysin. Siinä missä LDP-perustainen VPLS on hallinnaltaan lähinnä kokoelma VPWS:iä, on BGP-perustainen VPLS taas muistuttaa L3-VPN:ää ilman asiakkaan IP-osoitteiden kuljettamista.

2.7.4.1 PE-reititinten löytäminen

Aivan kuten VPWS:ssä, LDP-pohjaisessa VPLS:ssä käytetään lähtökohtaisesti staattista konfigurointia, jolloin PE-reititinten löytämistä ei tarvita. Myös samantapaisia automaattisen PE-reititinten löytämisen mekanismeja on ehdotettu kuin VPWS:lle. IETF:n L2vpn-työryhmän virallisessa – tosin työn alla olevassa – dokumentissa on määritelty ainoastaan BGP:n käyttö tähän tarkoitukseen. PE-reititinten löytämisen kannalta se on identtinen L3-VPN:n tavan kanssa. [Ros06b]

BGP-perustaisessa VPLS:ssä on sisäänrakennettuna L3-VPN:n tapainen PE-reititinten automaattisen löytämisen mekanismi. [Kom07]

2.7.4.2 Kuljetustunnelin valitseminen

Tietty PW on aina kytketty päättyväksi tiettyyn PE:hen. PE:n osoite on joko konfiguroitu tai löydetty edellä kuvatulla mekanismilla. Kuljetustunnelin valinta perustuu PW:n yhteydessä signaloituihin tietoihin. Leimakytkentäisessä verkossa tälle osoitteelle pitäisi löytyä kuljetusleima ja IP-tunnelointia hyödyntävässä verkossa vastaavasti tunneliliitäntä.

2.7.4.3 VPN-leimojen signalointi

VPN-leimojen signalointi tapahtuu eri VPLS-palveluissa eri protokollilla. RFC 4761:ssä VPN-leimat kuljetetaan BGP-signaloinnin mukana kuten RFC4364-palvelussa (vain eri osoiteperheen avulla). RFC 4762:ssa VPN-leimat välitetään PW:iden signaloinnin yhteydessä LDP-protokollan avulla.

2.7.4.4 VPN-signalointi

VPLS:ssä ei signaloida mitään virtuaaliverkon sisäisiä osoitetietoja. PE:iden VSI:iden kytkentätaulut perustuvat puhtaasti liikenteen tarkkailuun ja siitä tehtävään MAC-osoitteiden ja niiden sijaintien opiskeluun. Poikkeuksena on LDP-pohjaisen VPLS:n mahdollistama MAC-osoitteiden poisto toisten PE-reititinten VSI:den kytkentätauluista. Tähän on olemassa oma osoitteiden poisto –viestinsä. Tätä viestiä voi käyttää esimerkiksi tilanteessa, jossa yhteys PE:n ja CE:n välillä katkeaa. [Las07] [Kom07]

2.7.5 Yhteenveto virtuaalisesta lähiverkkopalvelusta

Jatkotyön kannalta olennaisimmat VPLS-palvelun ominaisuudet ja toiminnot ovat:

- VLPS-palvelu tarjoaa asiakkaalle usean toimipisteen yhdistämisen virtuaalisella Ethernet-lähiverkolla.
- VPLS olettaa, että PE-laitteiden välillä on kuljetustunnelit. Palvelu ei luo niitä.
- VLPS-palvelusta on julkaistu kaksi kilpailevaa standardiehdotusta (RFC 4761 ja RFC 4762).
- Ehdotuksilla on kolme merkittävää eroa:
    - Toinen käyttää virtuaalijohtimien luontiin BGP:tä (RFC 4761), toinen LDP:tä (RFC 4762).
    - Vain RFC 4762 määrittelee hierarkkisen VPLS:n.
    - Vain RFC 4761 sisältää mekanismin PE-reititinten automaattiseen löytämiseen, RFC 4762:ssä tämä on jätetty määrittellemättä.
- RFC4761: BGP:n käyttöön pätevät samat seikat kuin L3-VPN:n kohdalla (tunnistetiedot, tietojen leviäminen ja sen rajoittaminen).
- RFC4762: Jos BGP:tä käytetään PE-reititinten löytämiseen, siihen pätevät samat seikat kuin L3-VPN:n kohdalla (tunnistetiedot, tietojen leviäminen ja sen rajoittaminen).
- RFC4762: Jos PE-reititinten automaattista löytämistä ei käytetä, lähetetään VPN-signalointia vain sille PE:lle, joka on konfiguroitu kyseisen reitittimen vastapääksi.

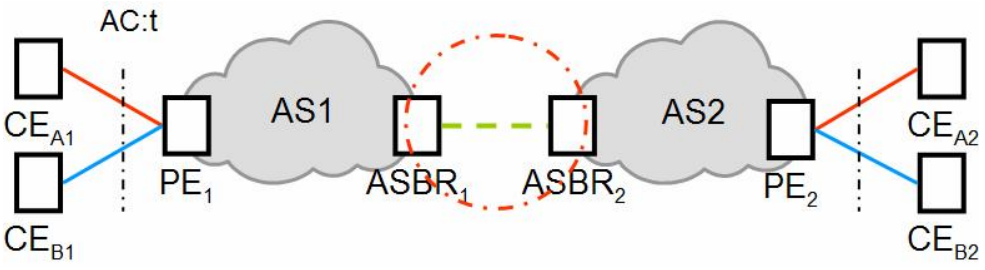
2.8 Eri virtuaaliverkkotyypit ja autonomisten alueiden yhteenliittäminen

Autonomisten alueiden yhteenliittäminen on otettu kirjavasti huomioon eri virtuaaliverkkopalveluissa. RFC 4634 on omistanut asialle oman kappaleen, muissa asiaa on käsitelty vaihtelevasti. IETF:n L2-työryhmä on jopa rajannut virallisesti toimivansa vain yhden AS:n kattavien ratkaisujen parissa [Iet07a]. Edellä mainituista syistä johtuen eri virtuaaliverkkopalvelut ovat eri lailla valmiita toimimaan yli autonomisten alueiden rajojen. Seuraavassa luvussa käsitellään erilaisia autonomisten alueiden liittämistapoja. Siinä käydään yksityiskohtaisesti läpi myös toteutus kaikkien tässä luvussa esiteltyjen virtuaaliverkkopalveluiden osalta.

luku 3:
Eri autonomisten alueiden virtuaaliverkkojen yhteenliittämistavat

Edellisessä luvussa kuvatut virtuaaliverkkopalvelut toimivat lähtökohtaisesti vain yhden autonomisen alueen sisällä. Jotta operaattorit voisivat tarjota virtuaaliverkkopalvelua, jossa asiakkaan toimipisteet ovat kytkettyinä eri verkkoihin, pitää virtuaaliverkkopalvelun toimia useamman autonomisen alueen ”yli”. Nämä eri verkot voivat kuulua joko samalle tai eri operaattorille: teknisesti tilanne on sama, mutta muuten vaatimukset saattavat poiketa toisistaan.

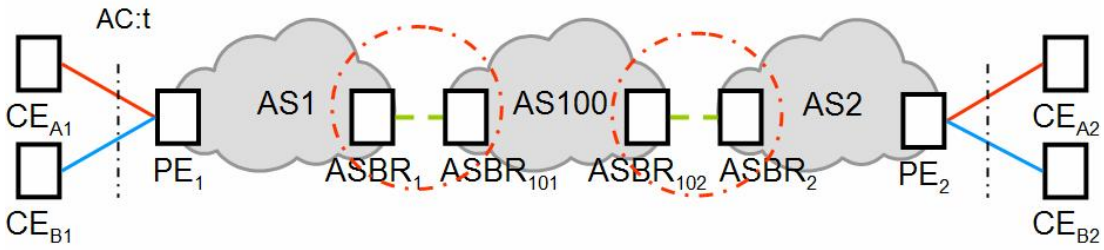
Tässä luvussa käsitellään neljää tapaa yhdistää kahdessa tai useammassa verkossa (AS:ssä) toteutetut virtuaaliverkkopalvelut. Kullekin tavalle on oma alalukunsa. Olen nimennyt tavat malleiksi A, B, C ja D. Nimeämisen innoittajana on ollut L3-VPN-dokumentti RFC4364 (tunnetaan myös nimellä RFC2547bis), jonka luvussa 10 on esitelty kolme tapaa (a, b ja c) liittää VPN yli AS-rajan. Koska tässä työssä käsitellään kahta muutakin MPLS-VPN:ää RFC4634:n lisäksi, olen laajentanut ”optioiden a, b ja c” kattavuutta myös näihin muihin VPN-palveluihin. Lisäksi mukaan on otettu neljäs yhteenliittämistapa (malli D).



Kuva 10. Kahden verkon liittäminen

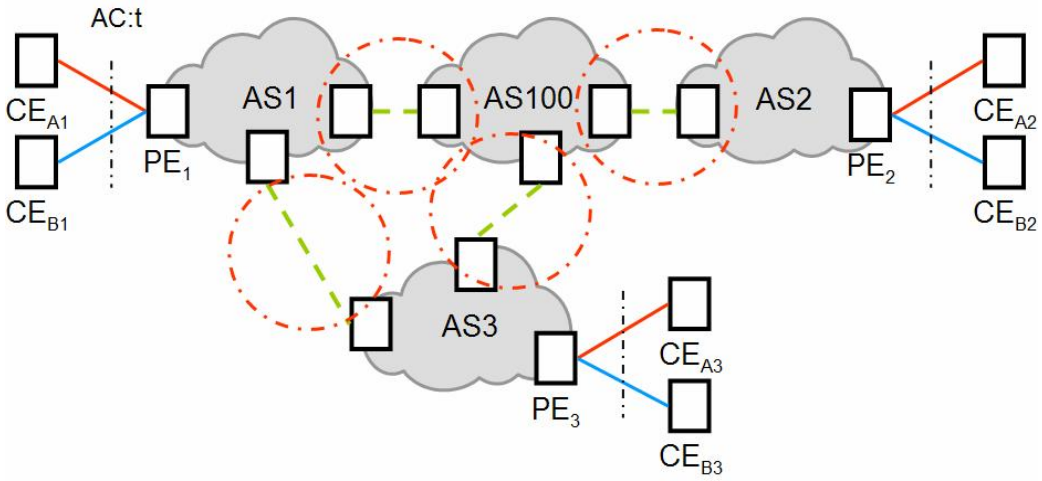
Yksinkertaisimmillaan yhteenliitettäviä AS:iä on kaksi, kuten kuvassa 10. Siinä on kaksi VPN-asiakasta (punainen ja sininen), joilla kummallakin on yksi toimipiste kytkettynä AS1:een ja yksi AS2:teen. AS:ien välillä voi olla myös kolmas operaattori.

Jos tällä ei ole omia PE-reitittimiä, sanotaan sitä transit-operaattoriksi (AS100 kuvassa 11).



Kuva 11. Yhteenliittäminen transit-operaattorin kautta

Yhteenliittymisten määrälle ei ole teknistä rajoitetta: operaattori voi liittyä yhteen niin monen operaattorin kanssa kuin se haluaa. Yhteenliittämistavat eivät myöskään ole toisistaan riippuvaisia: operaattori voi liittyä eri tavoin eri operaattoreihin. Tästä seuraa, että useammasta AS:tä voi muodostua hyvin monenlaisia AS-topologioita. Kuvassa 12 on esimerkki.



Kuva 12. Usean AS:n muodostama kokonaisuus

Koska yhteenliitettävien verkkojen määrän lisääminen ei sinällään vaikuta yksittäiseen liitäntään, käsitellään tästä eteenpäin vain kahden operaattorin välistä yhteenliittämistä. On kuitenkin hyvä huomioida, että operaattoreilla on tarve koordinoida tiettyjä asioita keskenään. Riippuen yhteenliittämistavasta, tällaisia asioita ovat esimerkiksi salausavaimet ja kohdesuotimien (RT) käyttö. Mitä useampia yhteenliitettäviä verkkoja on, sitä isompi tämä hallinnollinen tehtävä on ja sitä enemmän erilaisia konfigurointisääntöjä verkkoon tulee tehtäväksi. Tämä lisää myös virheiden mahdollisuutta ja sitä kautta voi heikentää tietoturvaa.

3.1 Standardoinnista

IETF:n työryhmät Pwe3 ja L3vpn ovat asettaneet tavoitteikseen kirjata vaatimuksia ja toteutustapoja useammassa autonomisessa alueessa toimiville virtuaaliverkoille, kun taas L2vpn on toistaiseksi rajannut kysymyksen työnkuvansa ulkopuolelle [Iet06][Iet07a][Iet07b]. Työryhmien työ ei kuitenkaan täysin noudata työkirjassa asetettuja tavoitteita. Niinpä yksittäisiä vaatimuksia ja toteutusehdotuksia inter-AS-toiminnallisuuksille löytyy kaikkien edellä mainittujen työryhmien joistakin dokumenteista. Yhtään pelkästään yhteenliittämiseen keskittyvää dokumenttia ei ole, vaan autonomisten alueiden yhteenliittämiseen liittyvät asiat ovat ripoteltuina eri dokumentteihin.

Käytännössä jo julkaistuissa RFC:issä on niukasti inter-AS-asiaa. Laajimmin viitattu dokumentti – L3-MGP/MPLS-VPN-palvelun määrittely [Ros06a] – esittelee päällisin puolin kolme eri tapaa toteuttaa inter-AS-rajapinta. Tätä hieman laajemmin asiaa on käsitelty toisessa VPLS-määrittelyistä [Kom07]. Siinä on käyty läpi RFC 4364:n mainitsemat kolme yhteenliittämisvaihtoehtoa BGP-signaloidun VPLS:n kannalta. Virtuaalijohtimien osalta IETF:n Pwe3-työryhmä on kehittelemässä moniosaisia (*engl. multi-segment*) virtuaalijohtimia, joiden eräs motivaattori on inter-AS-tarpeet [Boc06]. Edellisten lisäksi useissa palveluiden vaatimusdokumenteissa inter-AS-asiaa on käsitelty suhteellisen pintapuolisesti. [Aug06][Xia04][Nag04][Car05][Mor07][Bit06]

3.2 Yhteenliittämisen tavat

Palvelualustojen yhteenliittämistä voi ajatella kuvan 10 avulla. Kuvassa on kaksi erillistä verkkoa (AS1 ja AS2), joiden välissä on liityntäverkko. Verkot voidaan ajatella erillisiksi MPLS-VPN-palvelualustoiksi, joiden sisällä reuna- ja rajareitittimien (PE:t ja ASBR:t) välillä on olemassa kuljetustunnelit. Kuvassa on myös esitettynä kaksi asiakasta: Asiakas ”Punainen” (toimipisteet A_1 ja A_2) ja asiakas ”Sininen” (toimipisteet B_1 ja B_2).

Seuraavissa alaluvuissa (3.3-3.6) esitellään neljä eri tapaa liittää MPLS-VPN-palvelualueet yhteen (mallit A, B, C ja D). Näin muodostuu yhtenäinen palvelualusta virtuaaliverkkopalveluiden tarjoamiseen. Yhteenliittämistä tarkastellaan luvussa 2 esitellyille kolmellle virtuaaliverkkopalvelulle (L3VPN, VPWS ja VPLS).

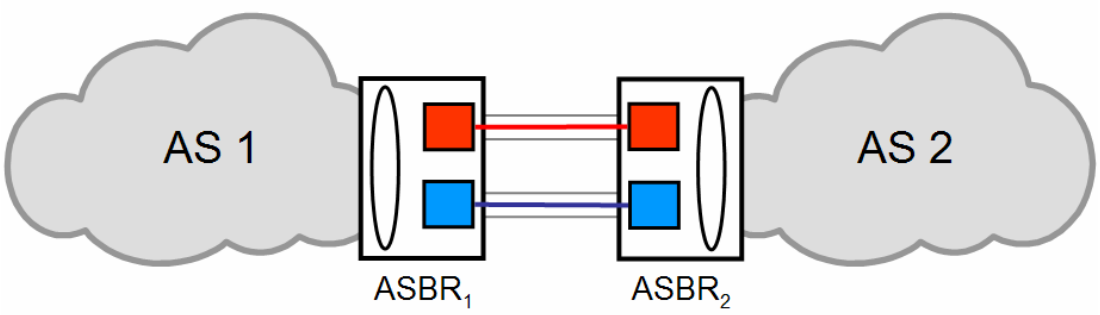
Luvussa 2 esiteltyjen virtuaaliverkkopalveluiden toteuttamisessa yli verkkorajojen on kolme teknistä kysymystä, jotka on ratkaistu eri yhteenliittämismalleissa eri tavoin. Nämä kysymykset ovat:

1. VPN-pakettien *välitys* eri autonomisissa alueissa olevien rajareititinten välillä.
2. VPN-yhteyksiin liittyvä *signalointi* eri virtuaaliverkkopalvelualustojen (autonomisten alueiden) välillä.
3. Virtuaaliverkkopalvelua tietylle asiakkaalle toteuttavien *reunareititinten löytäminen.*

Seuraavissa neljässä alaluvussa esittelen neljä eri tapaa muodostaa useamman verkon yli toimiva virtuaaliverkkopalvelu. Kukin alaluku on jaettu paketin välitys –osuuteen ja hallintasoon keskittyvään osuuteen. Hallintataso-osuus on edelleen jaettu virtuaaliverkkopalvelukohtaisiin osiin.

3.3 Malli A: Virtuaaliverkon muodostaminen manuaalisesti ketjuttamalla

Yksinkertaisin tapa yhdistää kaksi eri autonomisissa alueissa olevaa leimakytkentäistä virtuaaliverkkoa on esitetty kuvassa 13. Siinä VPN:t on ketjutettu käyttäen erillisiä siirtoyhteystason yhteyksiä kullekin virtuaaliverkolle rajareititinten (ASBR) välillä. Nämä siirtoyhteydet voivat olla joko erillisiä johtimia taikka loogisia yhteyksiä, riippuen ASBR:ien välissä olevasta liityntäverkosta. Tässä voidaan hyödyntää esimerkiksi Ethernet VLAN:eja.



Kuva 13. Malli A: Eri AS:issä olevien VPN:ien manuaalinen yhdistäminen erillisillä siirtoyhteyksillä

Mallilla A tehty virtuaaliverkkopalvelualustojen yhteenliittäminen ei vaadi kummaltakaan autonomiselta alueelta tukea perus-MPLS-VPN-toiminnallisuuden lisäksi: $ASBR_2$ näyttää $ASBR_1$:lle aivan CE-reitittimeltä ja päinvastoin[30]. Toiminnallisesti ASBR:t ovat mallissa A PE-reititimiä.

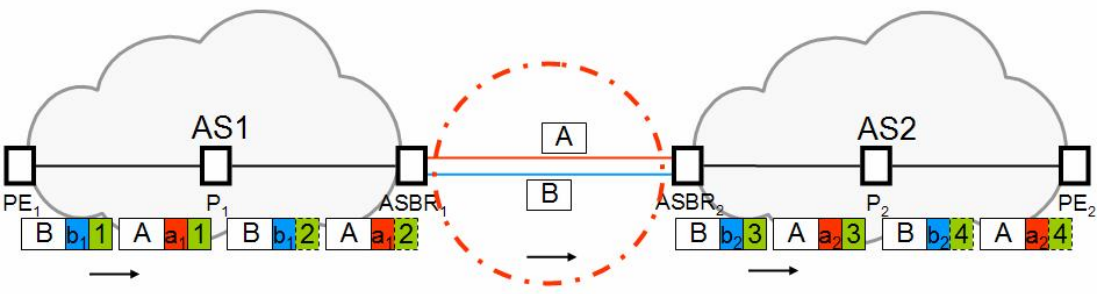
3.3.1 Pakettien välitys mallissa A

Mallin A pakettien välitys on kuvattu kuvassa 14. Kuvassa on vain toinen liikennesuunta (AS1→AS2), mutta toinen suunta toimii samoin. Kuvassa siniset ja punaiset leimat ovat VPN-leimoja, vihreät kuljetusleimoja. ASBR:ien välissä VPN-liikenne on leimaamatonta ja omilla ”johtimillaan”. Koska liikenne AS:ien välillä on leimaamatonta[31], joutuu ASBR2 sekä VPN- että kuljetusleimaamaan paketit.

---

[30] Oikeammin: kukin toisen verkon rajareitittimen VFI näyttää CE:ltä toisen AS:n ASBR:lle.

[31] Erikoistapauksessa, jossa L3-VPN on tyyppiä Carriers’ Carrier (käsitelty luvussa 2.6.1.1), voi liikenne olla mallissa A leimattua.



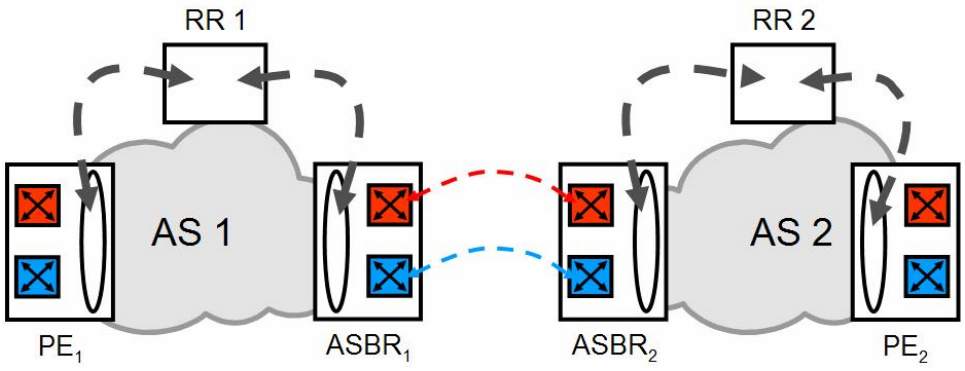
Kuva 14. Paketin kulku mallissa A

Koska VPN-liikenne menee ASBR:ien välissä leimaamattomana, pitää AS:ien välisen liityntäverkon tukea VPN-liikenteen ominaista liikennöintiä. L3-VPN:n tapauksessa tämä ei ole ongelma[32], mutta L2-VPN-palvelulle tämä asettaa rajoituksia, koska liityntäverkon pitää olla käytännössä samaa L2-tekniikkaa kuin yhteyden, jota L2-VPN emuloi.

3.3.2 Hallintataso mallissa A

3.3.2.1 L3-virtuaaliverkon hallintayhteydet mallissa A

Kuvassa 15 on esitetty miten RFC4364:n mukaiseen virtuaaliverkkopalveluun liittyvä signalointi tapahtuu mallin A mukaisessa verkkojen yhteenliittämisessä. Kuvasta näkyy, että ASBR:ien välillä ei ole VPN-signalointia (harmaat katkoviivat), mutta ASBR:issä olevien VFI:den välillä voidaan ajaa normaalia IP-signalointia (mitä tahansa laitteiden tukemaa IP-reititysprotokollaa). Jokaisella virtuaaliverkolla on oma, muista riippumaton, reititys. Tämä reititys muutetaan edelleen rajareitittimessä VPN-signaloinniksi, kuten PE-reitittimissä intra-AS-tapauksissa.



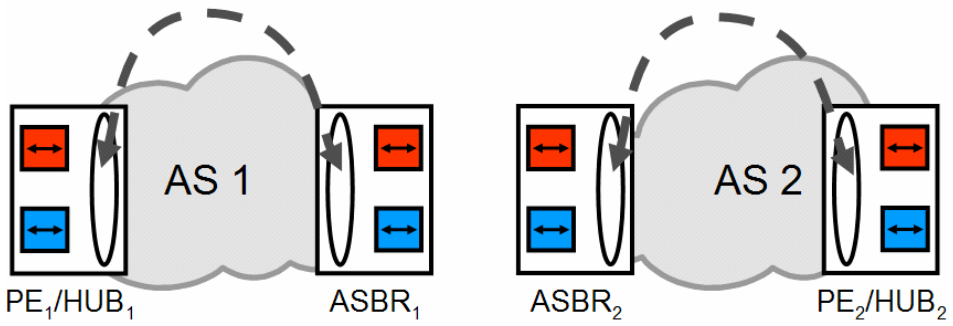
Kuva 15. L3-VPN-signalointi mallissa A

[32] IP-sovitus on tehty kaikille yleisille L2-tekniikoille.

Koska VPN-signalointia ei mallissa A vaihdeta AS:ien välillä, ei PE-reititinten automaattinen löytäminen onnistu kuin AS:n sisällä. Myöskään L3-VPN:ille ominaiset BGP-tunnisteet (RT, RD) eivät liiku verkkojen välillä. Malli A vaatii konfigurointia erikseen molemmissa AS:issä ja lisäksi niiden välisen yhteyden konfigurointia ja liittämistä oikeaan VPN:ään.

3.3.2.2 Virtuaalijohtimien hallintayhteydet mallissa A

Kuvassa 16 on esitetty, miten VPWS-palveluun liittyvä signalointi tapahtuu mallin A mukaisessa verkkojen yhteenliittämisessä. Kuvasta näkyy, että ASBR:ien välillä ei ole mitään signalointia. Myöskään PE-reititinten automaattinen löytäminen ei onnistu mallissa A, vaan se vaatii konfigurointia erikseen molemmissa AS:issä ja lisäksi niiden välisen yhteyden konfigurointia ja liittämistä oikeaan VPN:ään.



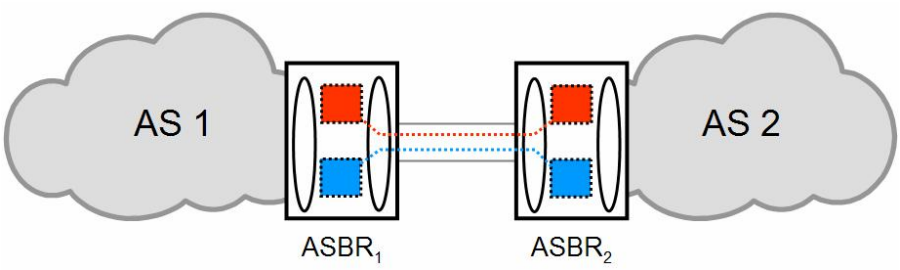
Kuva 16. Virtuaalijohtimien signalointi mallissa A

3.3.2.3 Virtuaalinen lähiverkkopalvelu mallissa A

Mallissa A kummankaan – BGP- tai LDP-perustaisen – VPLS-palvelun hallintayhteyksiin ei liity signalointia AS:ien välillä (kuten VPWS:ssä, kuva 16). Ethernetin oma signalointi (kuten Spanning Tree –protokolla tai Ethernet OAM) toimii kuitenkin ASBR:ien VSI:den välillä. Myöskään PE-reititinten automaattinen löytäminen ei onnistu mallissa A, vaan se vaatii konfigurointia erikseen molemmissa AS:issä ja lisäksi niiden välisen yhteyden konfigurointia ja liittämistä oikeaan VPN:ään.

3.4 Malli B: Virtuaaliverkon muodostaminen VPN-tason yhdistämisen avulla

Mallin B mukainen tapa yhdistää kaksi eri autonomisissa alueissa olevaa leimakytkentäistä virtuaaliverkkoa on esitetty kuvassa 17. Siinä on yhteinen siirtoyhteystason yhteys kaikille VPN:ille ASBR:ien välillä. Tämä yhteys voi olla mitä tahansa L2-tekniikkaa, jolla voidaan kuljettaa MPLS-leimattua liikennettä.



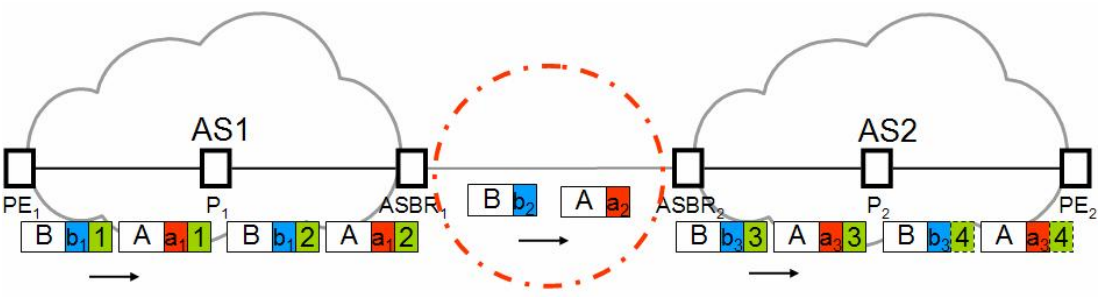
Kuva 17. Malli B: Looginen VPN-tason yhdistäminen

Mallilla B virtuaaliverkkopalvelualustojen yhteenliittäminen vaatii perus-MPLS-VPN-toiminnallisuuden lisäksi tukea ASBR-reitittimiltä. Niiden pitää toimia sekä VPN-signaloinnin välityspisteinä että sen hyödyntäjinä. Rajareitittimien pitää osata myös kytkeä paketteja VPN-leimojen perusteella kahden leimakytketyn liitännän välillä[33].

3.4.1 Pakettien välitys mallissa B

Mallin B pakettien välitys on kuvattu kuvassa 18. Kuvassa on vain toinen liikennesuunta (AS1→AS2), mutta molemmat suunnat toimivat samoin. Kuvassa siniset ja punaiset leimat ovat VPN-leimoja, vihreät kuljetusleimoja. ASBR:ien välissä paketeilla on vain VPN-leima, jonka perusteella $ASBR_2$ osaa liittää paketin oikeaan VPN:ään (ja edelleen kuljetustunneliin).

[33] Tätä voi ajatella laajennettuna PE-reitittimen toimintana. Normaali PE kytkee paketteja leimaamattomalta AC:ltä leimattuun runkoverkkoon ja toisinpäin.



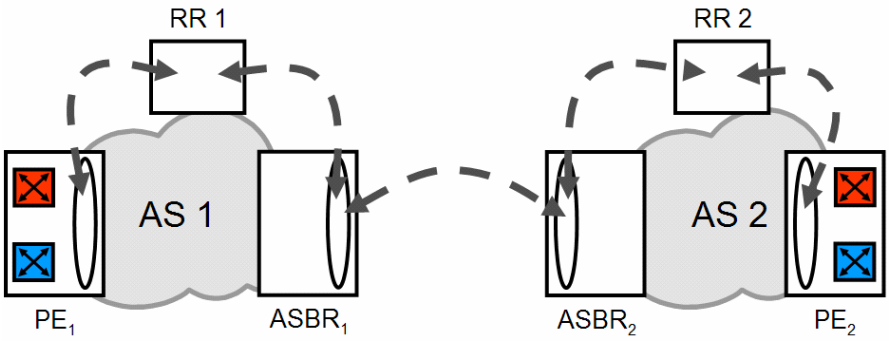
Kuva 18. Paketin kulku mallissa B

Koska liikenne kulkee AS:ien välillä leimattuna, ei AS:ien välisen liitäntäverkon tekniikalla ole vaikutusta siihen, mitä VPN-liikennettä pystytään kuljettamaan.

3.4.2 Hallintataso mallissa B

3.4.2.1 L3-virtuaaliverkon hallintayhteydet mallissa B

Kuvassa 19 on esitetty miten RFC4364:n mukaiseen virtuaaliverkkopalveluun liittyvä signalointi tapahtuu mallin B mukaisessa verkkojen yhteenliittämisessä. Kuvasta näkyy, että ASBR:ien välillä on BGP:hen perustuva VPN-signalointiyhteys. Erotuksena autonomisen alueen sisäisestä iBGP-yhteyksistä, tämä yhteys on eBGP-yhteys, minkä johdosta ASBR1 muuttaa itsensä toiseen verkkoon mainostettavien VPN-reittien seuraavaksi hypyksi (engl. next-hop). Näin ASBR2 osaa lähettää liikenteen AS1:een, vaikkei sillä olisikaan reittiä ja leimaa reitin oikeaan alkuperään (PE1).



Kuva 19. BGP-signalointi L3-VPN:lle mallissa B

Koska mallissa B VPN-signalointi liikkuu autonomisten alueiden välillä kutakuinkin samoin kuin autonomisen alueen sisällä, välittyy kaikki L3-VPN-signalointi toiseen AS:ään, ellei sitä erikseen rajoiteta. Rajoituskeinoja on kahta eri tyyppiä: joko pidetään huolta, ettei ASBR1:lle mene muuta VPN-signalointia kuin AS2:teen tarkoitettua tai suodatetaan ASBR1:ssä muu kuin AS2:een tarkoitettu. Ensimmäinen tarkoittaa joko suodattamista RR:ssä tai erillista laitteistoa inter-AS-VPN:ille.

Erillinen laitteisto[34] on verkkoarkkitehtonisesti selkeä vaihtoehto, mutta usein liian kallis ja jäykkä[35]. Lisäksi, jos kumppani-AS:iä on useampia, tarvittaisiin näille kaikille mahdollisesti erilliset laitteistot.

Käytettäessä samaa laitteistoa sekä intra- että inter-AS-VPN:ille, tarvitaan helppo keino suodattaa reititystä kohde-AS-kohtaisesti. Koska L3-VPN:ssä on olemassa jo VPN-suodatukseen käytettävä parametri kohdesuodin (RT), on sen käyttö myös AS-kohtaiseen suodatukseen luontevaa. Tarvittavien konfiguraatiomuutosten ja AS:ien (operaattoreiden) välisen koordinointitarpeen minimoimiseksi on järkevintä ottaa käyttöön varsinaisista asiakaskäyttöön tarkoitetuista reittisuotimista erilliset RT:t vain AS:ien välistä suodatusta varten. Tähän ”inter-AS-RT:hen” operaattori voi koodata esimerkiksi kohde-AS:n jollain tavalla (ei kuitenkaan varsinaiseen AS-kenttään, sillä siihen saa laittaa vain oman AS:nsä). Tällainen malli on erityisen käyttökelpoinen liitettäessä useita AS:iä yhteen.

Mallissa B ei varsinaisesti löydetä toisessa AS:ssä olevaa kohde-PE:tä, vaan omassa verkossa oleva ASBR, joka ”näyttää” kohde-PE:ltä ja välittää liikenteen edelleen kohti kohde-PE:tä. Automaattisen VPN:n muodostumisen kannalta palvelu kuitenkin toimii samoin kuin yhden AS:n sisällä.

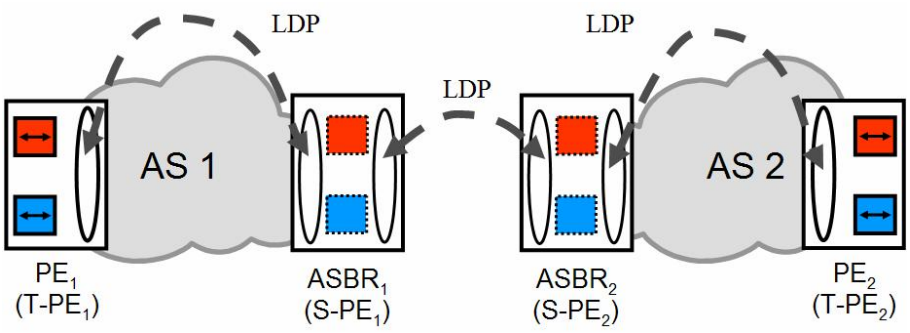
3.4.2.2 Virtuaalijohtimien hallintayhteydet mallissa B

RFC 4447 määrittelmä virtuaalijohtimien signalointi LDP-protokollalla ei sellaisenaan sovellu malliin B. IETF:n Pwe3-työryhmä on kuitenkin parhaillaan kehittämässä moniosaista (*engl. multi-segment*) virtuaalijohdinta, jossa ASBR voisi toimia ns. S-PE:nä (*engl. PW Switching Provider Edge*) [Boc06]. Tämän hetkisen dokumentin perusteella varsinaiset inter-AS:ään liittyvät asiat jäävät erilliseen dokumenttiin [Mar07]. Kuvassa 20 on esitelty moniosaisen virtuaalijohtimen signalointi. Siinä ASBR:ien välillä on LDP-yhteys virtuaalijohtimien luomista ja purkamista varten. Moniosaista PW:tä varten on määritelty omia TLV-laajennuksiaan, joiden tarkka käyttö on tässä vaiheessa vielä avoin. Tarkoituksena on kuitenkin hyödyntää tarkemmin määrittelemättömiä yksilöllisiä tunnisteita VPN-kohtaisille toistininstansselle sekä T-PE:issä (PE, johon asiakasyhteys on kytketty). *Engl. PW Terminating Provider Edge*) että S-PE:issä. Näitä voidaan hyödyntää sekä PE-reititinten automaattisessa löytämisessä että moniosaisten virtuaalijohtimien dynaamisessa signaloinnissa [Mar07].

---

[34] Erillinen laitteisto tarkoittaa tässä erillistä reittiheijastinta ja erillisiä PE-reitittimiä.

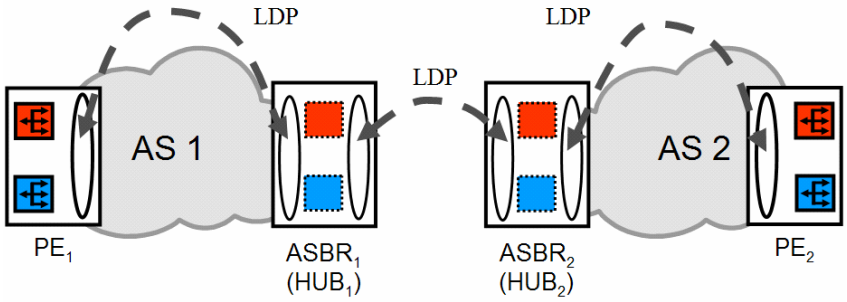
[35] Erillinen laitteistot vaatii asiakkaiden siirtämistä, kun intra-AS-VPN:t laajenevat yli AS-rajan.



Kuva 20. LDP-signalointi moniosaiselle virtuaalijohdimelle mallissa B

3.4.2.3 Virtuaalinen lähiverkkopalvelu mallissa B

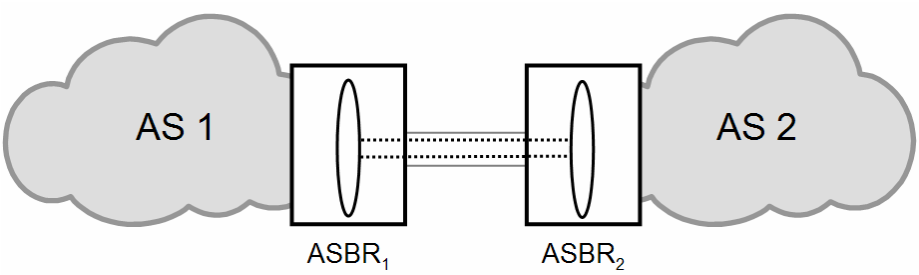
Mallissa B molempien VPLS-palveluiden (BGP- ja LDP-perustaisen) hallintayhteyksiin liittyy signalointia AS:ien välillä. LDP-pohjaisen VPLS:n signalointi on esitetty kuvassa 21. Malli B edellyttää LDP-VPLS:ltä hierarkkisen VPLS:n käyttöä ja sitä, että ASBR toimii sen hubina (virtuaalijohtimen pitää päättyä suoraan naapuriin, sillä mallissa B ei ole kuljetustunnelia AS:ien välillä). Toinen vaihtoehto olisi hyödyntää VPWS:n yhteydessä esiteltyjä moniosaisia vituaalijohtimia VPLS:n VSI:iden välillä. BGP:hen perustuvassa VPLS:ssä inter-AS-toiminta toimii mallissa B samoin kuin aiemmin esitellyllä L3-VPN:llä. [Kom07][Las07].



Kuva 21. LDP-signalointi VPLS:lle mallissa B

3.5 Malli C: Virtuaaliverkon muodostaminen leimakytkentäisen kuljetustason yhdistämisellä

Mallin C mukainen tapa yhdistää kaksi eri autonomisissa alueissa olevaa leimakytkentäistä virtuaaliverkkoa on esitetty kuvassa 22. Siinä ASBR:ien välillä on leimakytkentäinen yhteys, jota kuljetustunnelit voivat käyttää. ASBR voidaan konfiguroida suodattamaan mainostamansa leimalliset reitit niin, että vain haluttuihin PE-reitittimiin johtaa leimakytketty polku toisesta AS:stä[36].



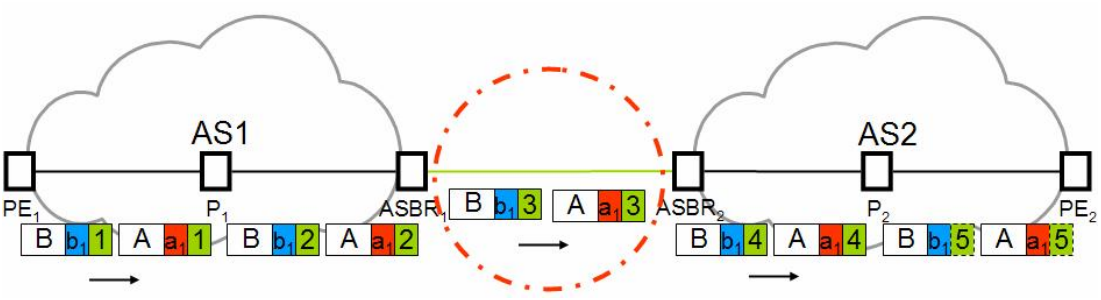
Kuva 22. Malli C: leimakytkentäisen kuljetustason yhdistäminen

Malli C vaatii perus-MPLS-VPN-toiminnallisuuden lisäksi tukea ASBR-reitittimiltä ja reittiheijastimelta. ASBR:n tulee osata mainostaa leimattuja reittejä BGP-MP:llä ja reittiheijastimen tulee osata välittää VPN-reittejä iBGP:n lisäksi eBGP:llä. [Ros06a]

3.5.1 Pakettien välitys mallissa C

Mallin C pakettien välitys on esitetty kuvassa 23. Kuvassa on vain toinen liikennesuunta (AS1→AS2), mutta molemmat suunnat toimivat samoin. Kuvassa siniset ja punaiset leimat ovat VPN-leimoja, vihreät kuljetusleimoja. Paketeilla on koko matkan $PE_1 \rightarrow PE_2$ kuljetusleima.

[36] Mainostaminen ei ole sama kuin käytössä oleva. Mainostamatonkin reitti ja leima saattavat toimia, jos ne ovat olemassa.



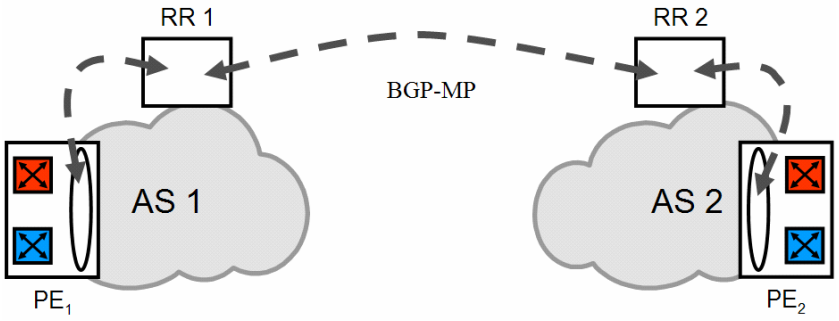
Kuva 23.Paketin kulku mallissa C

Koska liikenne kulkee AS:ien välillä leimattuna, ei AS:ien välisen liitäntäverkon tekniikalla ole vaikutusta siihen, mitä VPN-liikennettä pystytään kuljettamaan.

3.5.2 Hallintataso mallissa C

3.5.2.1 L3-virtuaaliverkon hallintayhteydet mallissa C

Kuvassa 24 on esitetty miten RFC4364:n mukaiseen virtuaaliverkkopalveluun liittyvä signalointi tapahtuu mallin C mukaisessa verkkojen yhteenliittämisessä. Kuvasta näkyy, että RR:ien välillä on BGP:hen perustuva VPN-signalointiyhteys. Erotuksena autonomisen alueen sisäisestä iBGP-yhteyksistä, tämä yhteys on eBGP-yhteys. RR_1 ei muuta toiseen verkkoon mainostettavien VPN-reittien seuraavan hypyn osoitetta, koska toisenkin verkon laitteilla pitäisi olla suoraan leimakytketty polku (kuljetustunneli) PE_1:een.



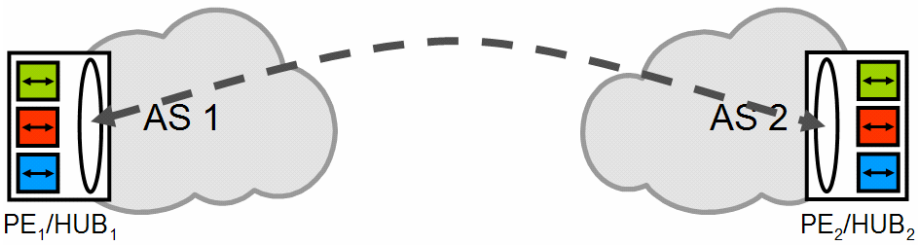
Kuva 24. BGP-signalointi L3-VPN:lle mallissa C

Samat signaloinnin rajoittamista koskevat pohdinnat koskevat mallia C, jotka käytiin läpi mallin B kohdalla L3-VPN-signalointiin liittyen (”inter-AS-kohdesuotimen” käyttö).

Mallissa C automaattinen PE-reititinten löytäminen tapahtuu BGP:n avulla aivan kuin intra-AS-palvelussa.

3.5.2.2 Virtuaalijohtimien hallintayhteydet mallissa C

RFC 4447 määrittelmä virtuaalijohtimien signalointi LDP-protokollalla soveltuu sellaisenaan malliin C (kuva 25). Jos halutaan aggregoida yhteyksiä verkkojen välillä, voidaan hyödyntää moniosaisia virtuaalijohtimia [Mar07]. Mallissa C tämä keskittävä komponentti (S-PE) voi sijaita muuallakin kuin rajareitittimessä.



Kuva 25. LDP-signalointi virtuaalijohtimelle mallissa C

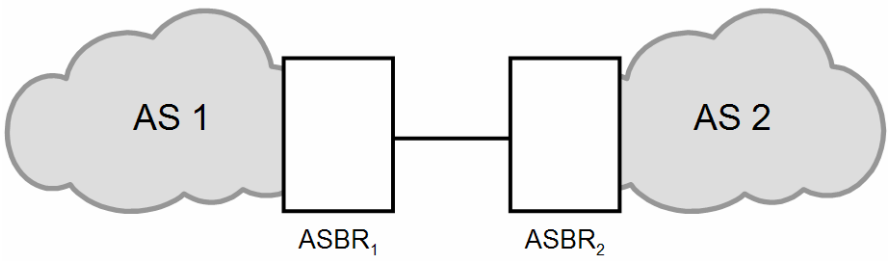
3.5.2.3 Virtuaalinen lähiverkkopalvelu mallissa C

Sekä RFC 4761:ssä että RFC 4762:ssa määritellyt virtuaaliset lähiverkkopalvelut soveltuvat sellaisenaan malliin C. RFC:n 4761 mukaisen palvelun signalointi toimii samalla lailla kuin L3VPN:ssä (kuva24) ja RFC 4762:n vastaavasti samalla lailla kuin virtuaalijohtimessa (kuva 25). Jos RFC 4762:n mukaisessa palvelussa halutaan aggregoida yhteyksiä verkkojen välillä, voidaan hyödyntää H-VPLS:ää. Malli C:ssä hubin voi sijoittaa muuallekkin kuin ASBR:ään.

3.6 Malli D: Virtuaaliverkkojen yhdistäminen ilman leimakytkentää tukevien runkoverkkojen hyödyntämistä

Joskus PE-reititinten välille ei voida tai haluta luoda yhteyttä, jota pitkin leimatut paketit pääsevät kulkemaan, millään edellä mainituista malleista A, B tai C. Näin on esimerkiksi silloin, kun jostain reitillä olevasta verkosta puuttuu leimakytkentä kokonaan. Tällaisia tilanteita varten on kehitetty IP-tunnelointiin perustuvia menetelmiä kuljettaa MPLS-VPN-liikennettä. Tähän voidaan käyttää esimerkiksi GRE- tai IPsec-tunneleita [Wor05][Rek07] [Ros05].

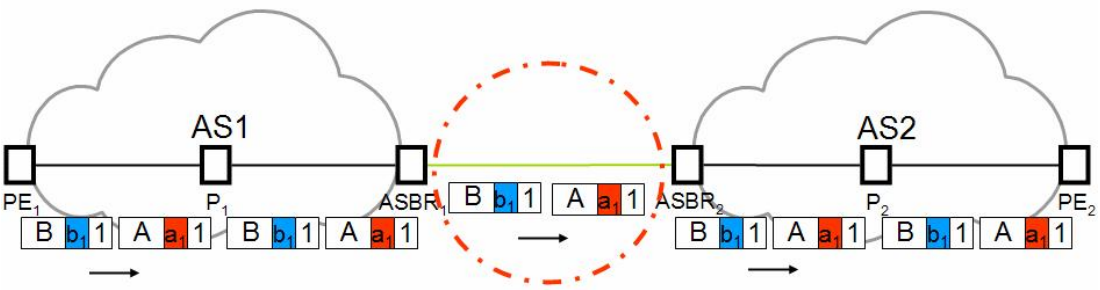
Käytettäessä jotain IP-tunnelointia suoraan PE-reititinten välillä, riittää ASBR:ien välillä normaali IP-tason yhteys (kuva 26). Käytettäessä tunnelointia tulee tunnelin päätepisteen varmistamiseen kiinnittää erityistä huomiota. Jos voi olla varma, että verkkoon ei pääse väärennetyillä osoitetiedoilla varustettuja paketteja, riittää osoiteperustainen suodatus. Muuten on käytettävä IPsec-suojattua tunnelointia. [Wor05]



Kuva 26. Malli D: verkkojen välillä vain IP-yhteys

3.6.1 Pakettien välitys mallissa D

Pakettien välitys mallissa D tapahtuu normaalin IP-reitityksen mukaisesti (kuva 27). IP-tunnelointia käytettäessä eivät leimakytkennän suomat liikenteen hallinnan (TE) keinot ole käytettävissä. [Wor05]



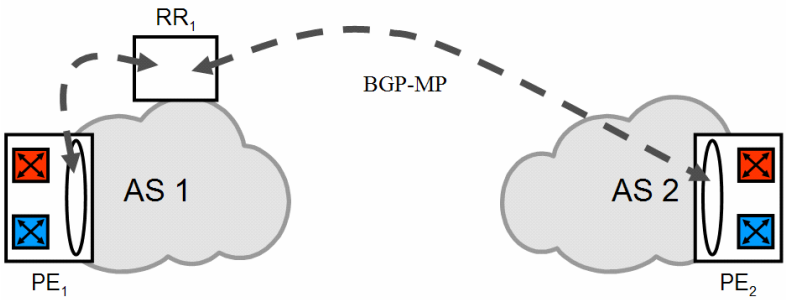
Kuva 27. Paketin kulku mallissa D

3.6.2 Hallintataso mallissa D

Malli D ei edellytä toimiakseen operaattorien välistä yhteistyötä normaalia Internet-liitäntää enempää[37]. Tästä syystä se on esitetty tässä mallina ”yksinäiselle sudelle” eli operaattorille, joka tekee kaiken VPN:iin liittyvän itse[38]. Näin ollen VPN-signalointia ei harrasteta toisen operaattorin kanssa, vaan suoraan PE-laitteisiin.

3.6.2.1 L3-virtuaaliverkon hallintayhteydet mallissa D

Kuvassa 28 on esitetty miten RFC4364:n mukaiseen virtuaaliverkkopalveluun liittyvä signalointi tapahtuu mallin D mukaisessa verkkojen yhteenliittämisessä. BGP:hen perustuva signalointiyhteys on suoraan reittiheijastimelta PE:lle. Samat signaloinnin rajoittamista koskevat pohdinnat koskevat mallia D, jotka käytiin läpi mallin C kohdalla L3-VPN-signalointiin liittyen (”inter-AS-kohdesuotimen” käyttö). Mallissa D automaattinen PE-reititinten löytäminen tapahtuu BGP:n avulla aivan kuin intra-AS-palvelussa.



Kuva 28. BGP-signalointi L3-VPN:lle mallissa D

---

[37] Haluttaessa taata palvelun laatua tilanne luonnollisesti muuttuu.

[38] Todennäköisempi käyttö mallilla D on olla tukemassa malleja A, B tai C yhteyksillä, joilla niiden käyttö ei ole mahdollisia.

3.6.2.2 Virtuaalijohtimien hallintayhteydet mallissa D

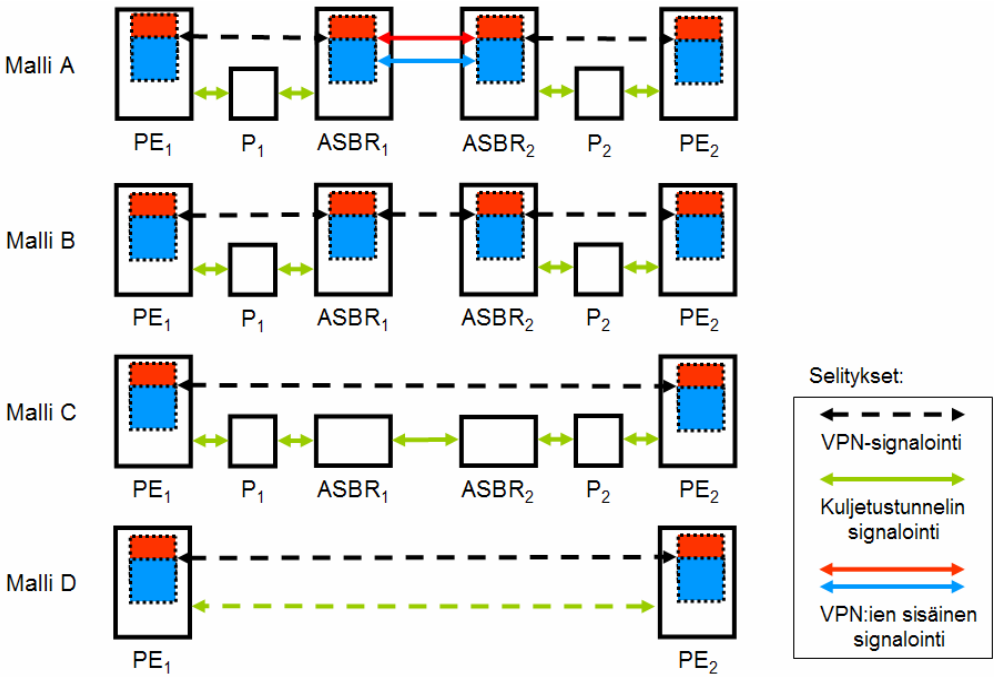
RFC 4447 määrittelemä virtuaalijohtimien signalointi LDP-protokollalla soveltuu sellaisenaan malliin D samoin kuin malliin C.

3.6.2.3 Virtuaalinen lähiverkkopalvelu mallissa D

Sekä RFC 4761:ssä että RFC 4762:ssa määritellyt virtuaaliset lähiverkkopalvelut soveltuvat sellaisenaan malliin D samoin kuin edellä käsiteltyyn malliin C.

3.7 Yhteenveto

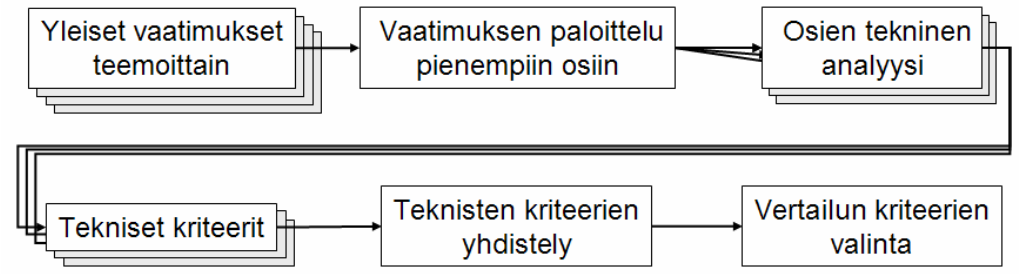
Olen tehnyt kuvaan 29 yleisesityksen kaikista alaluvussa 3.2 esitellyistä neljästä eri yhteenliittämismallista. Olen kuvannut vain hallintaan käytetyt signaloinnit yleisellä tasolla. Olen jättänyt pois mahdolliset palveluspesifiset signaloinnit ja laitteet. Kuva havainnollistaa erityisesti rajareitittimen erilaista roolia eri malleissa. Koska iso osa verkkojen yhteenliittämiseen liittyvistä tietoturvauhista on perinteisesti hoidettu rajalaitteen signaloinnin ja liikenteen hallinnan avulla, on rajareitittimen rooli myös virtuaaliverkkopalveluita yhteenliitettäessä keskeinen.



Kuva 29. Yleiskuva kaikkien yhteenliittämistapojen hallintatasoista

luku 4:
Vertailun kriteerit

Tässä luvussa esittelen vertailun kriteerit, joiden perusteella teen seuraavan luvun (5) vertailun. Olen muodostanut kriteerit kuvan 30 mukaisesti lähtien yleisluontoisista vaatimuksista ja päätyen tarkkoihin kriteereihin. Tätä prosessia olen selvittänyt alaluvussa 4.1. Vertailuun valitut yhdistellyt kriteerit on koottu alaluvun 4.7 taulukkoon 6. Yleisluontoisten vaatimusten taustoja tuon esille alaluvussa 4.2.



Kuva 30. Vaatimuksista vertailun kriteereiksi

Vertailun kriteerit sekä tuovat vaihtoehtoisten yhteenliittämistapojen olennaiset piirteet esille että helpottavat vaihtoehtojen vertailua keskenään. Yksityiskohtaisten vertailukriteerien laajemmat tekniset taustat löytyvät tämän työn edellisistä luvuista. Kriteerien valintaan vaikuttavat tässä työssä esitetyn kirjallisen selvityksen lisäksi omassa työssäni operaattorin palveluksessa havaitsemani haasteet liittyen useammassa verkossa toimiviin leimakytkentäisiin virtuaaliverkkoihin. Pyrin tuomaan nämä kriteerien valintaan vaikuttaneet seikat tulevissa alaluvuissa esille.

4.1 Kriteerien valintamenettelystä

Olen valinnut vertailun kriteerit ylhäältä alas –metodilla. IETF on julkaissut virtuaaliverkkojen tietoturvallisuusvaatimuksista dokumentin ”*Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)*” [Fan05]. Dokumentissa on listattu tietoturvallisuuteen liittyviä asioita, joita virtuaaliverkkopalvelua suunniteltaessa tulisi ottaa huomioon. Olen käyttänyt RFC 4111:n listaamia asioita perustana omille ”yleisille vaatimuksilleni”.

RFC 4111 vain sivuaa verkkorajapinnan ylittäviä virtuaaliverkkoja eikä käsittele virtuaaliverkkojen teknisiä toteutuksia. Tässä työssä tarvittavaa tietoturvavaatimusten tarkempaa analyysia virtuaaliverkkotekniikoiden suhteen on tehty jonkin verran itse palveluiden määrittelydokumenteissa [Ros06a][Kom07][Las07] ja BGP/MPLS IP -VPN:ien osalta myös dokumentissa ”*Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)*”[Beh06]. Lukuun ottamatta RFC 4381:tä ei edellä mainituissa käsitellä autonomisten alueiden yhteenliittämisen vaatimuksia kuin pintapuolisesti, turvallisuusvaatimusten kannalta ei lainkaan. RFC 4381:ssä on oma alalukunsa turvallisuusnäkökulmille, jotka liittyvät BGP/MPLS IP -VPN:ien inter-AS-yhteenliittämiseen. Käytännössä olen tehnyt teknisen analyysin seuraavissa alaluvuissa L2-VPN:ien osalta autonomisten alueiden yhteenliittämiseen liittyen kokonaan itse ja L3-VPN:n osalta RFC 4381:een tukeutuen. Kriteerien yhdistämisen, koskemaan kaikkia työhön valittuja virtuaaliverkkopalveluita, olen tehnyt myös itse.

RFC 4111:een perustuvista yleisluontoisista vaatimuksista olen kuvan 30 mukaisesti työstänyt konkreettiset – varsin tekniset – kriteerit vertailulle. Olen katsonut tämän parhaaksi tavaksi saada vertailuun tarpeeksi laaja näkökulma. Jos olisin lähtenyt kasaamaan kokonaisvaltaista vertailua yksittäisistä teknisistä kriteereistä, olisi vaarana ollut, että vertailu painottuu asioihin, jotka ovat sillä hetkellä ajankohtaisia, ja muut – mahdollisesti yhtä merkittävät – olisivat jääneet liian vähälle huomiolle. Osa yksittäisistä kriteereistä on kuitenkin sellaisia, joita en ole johtanut edellä kuvatun mallin mukaisesti, vaan ne ovat tulleet vastaan joko IETF:n dokumenteissa tai työssäni operaattorin palveluksessa. Kriteerien valintaan ovat lisäksi vaikuttaneet näkemäni MPLS-VPN-aiheiset seminaariesitelmät ja sähköpostilistat, joiden viesteissä aihetta on sivuttu. Nämäkin kriteerit on esitetty tässä työssä ikään kuin ne olisivat tulosta samanlaisesta yleisestä yksityiseen -päättelystä. Tähän on kaksi syytä: ensinnäkin se helpottaa luettavuutta ja toiseksi se asettaa kaikki kriteerit samaan kontekstiin ja mittasuhteeseen muiden kriteerien kanssa.

4.2 Rajaus ja näkökulma

Keskityn tässä työssä leimakytkentää hyödyntävien virtuaaliverkkojen yhdistämisen haasteisiin, en *yleisesti* virtuaaliverkkopalveluiden ongelmiin enkä myöskään pakettiverkkojen tai IP-liikenteen yhteenliittämisen haasteisiin. Työssä keskitytään tietoturvallisuuteen liittyviin asioihin, koska se on keskeinen virtuaaliverkkoihin liitetty ominaisuus. Tietoturvalla myös perustellaan joidenkin yhteenliittämistapojen valintaa. Rajaus on tehty myös, jotta työ pysyisi selkeänä ja diplomityön laajuisena.

Tarkastelen leimakytkentäisten virtuaaliverkkojen liittämistä useamman autonomisen alueen yli *ensisijaisesti virtuaaliverkkopalvelun tarjoamisen ja sen mahdollistavan verkon näkökulmasta*. Tästä ”operaattorinäkökulmasta” muutos on varsin iso: MPLS-VPN:t ovat olleet pääasiassa yhden operaattorin yhdessä verkossa tuottamia palveluita. Sekä tekninen toteutus että toteutuksen taustalla oleva ajattelunmalli ovat perustuneet yhden autonomisen alueen sisällä toimimiseen. Virtuaaliverkkopalvelun näkökulmasta kyseessä on lähinnä olemassa olevien palveluiden maantieteellisen kattavuuden laajennus; yhteenliittämistapa saattaa kuitenkin aiheuttaa rajoituksia palveluille. Myös palvelunäkökulma on huomioitu kriteerien valinnassa, mutta olen korostanut operaattorinäkökulmaa.

4.3 Tietoturvallisuuteen liittyvät vaatimukset

Tietoturvallisuus on tärkeä ja kiinteä osa operaattorin tarjoamia virtuaaliverkkopalvelutekniikoita sekä VPN-asiakkaille että -palvelun tarjoajille. Olen tässä työssä laskenut RFC 4111:sta listattujen asioiden lisäksi myös *palvelun yksityisyyteen* ja *strategisiin tietoihin* liittyvät asiat turvallisuusasioihin kuuluviksi.

Olen jaotellut tietoturvallisuuteen liittyvät aiheet kahteen: *operaattoria koskeviin* ja *virtuaaliverkon käyttäjää (asiakasta) koskeviin*. Nämä täydentävät toisiaan, sillä *virtuaaliverkon turvallisuuden perustana on aina palveluntarjoajan verkon ja järjestelmien tietoturvallinen ylläpitäminen ja hallinta*. Asiakkaan täytyy voida luottaa operaattoriinsa (tai operaattoreihinsa). RFC 4111 esittelee käsitteen luottamusalue (*zone of trust*). Määritelmän mukaan kukin virtuaaliverkko on oma luottamusalueensa, ja runkoverkko, joka palvelun tarjoaa, on lisäksi oma luottamusalueensa [Fan05]. RFC 4111:ssä tarkastellaan vain uhkia, jotka tulevat turvallisuusalueen ulkopuolelta, alueen sisäisiä ongelmia ei käsitellä, sillä VPN-palveluiden ei ajatella poikkeavan normaaleista pakettiverkoista ”sisäisiltä” osin. Toisin sanoen normaalit IP- ja Ethernet-verkkojen tietoturvakäytännöt ovat sellaisenaan sovellettavissa sekä virtuaaliverkkopalvelun avulla toteutetulle

tietoverkolle että IP/MPLS-verkoille, jotka tarjoavat MPLS-perustaisia virtuaaliverkkoja palveluinaan.

Tämän työn kannalta haasteellinen on RFC 4111:n määrittely, jonka mukaan VPN-palveluita tarjoava runkoverkko on yksi luottamusalue, vaikka sen muodostaisi useampi operaattori [Fan05]. Asiakkaan, jolla on toimipisteitä useampaan autonomiseen alueeseen liitettynä, kannalta RFC 4111:n määritelmä on pätevä, mutta se jättää huomiotta sekä operaattorin että asiakkaat, joilla ei ole toimipisteitä liitettyinä useampaan AS:ään. Olenkin jakanut virtuaaliverkkopalveluiden käyttäjät kahteen ryhmään: Niihin, joilla on toimipisteitä useammassa AS:ssa (ns. inter-AS-asiakas) ja niihin, joilla ei ole (ns. intra-AS-asiakkaat). Tämä jaottelu näkyy selkeämmin vertailussa (luku 5) kuin tämän luvun kriteereissä.

Liitettäessä useampia verkkoja yhteen kasvaa ”runkoverkon” operaattorien määrä. Miten tämä vaikuttaa tietoturvallisuuteen, riippuu operaattoreista, niiden määrästä ja yhteenliittämistavasta. Joka tapauksessa asiakkaan, jonka virtuaaliverkon liikenne kulkee useamman operaattorin kautta, tulee voida luottaa näihin kaikkiin (tästä seuraa myös, että asiakkaan on hyvä tietää minkä verkkojen kautta hänen liikenteensä kulkee). Toisaalta asiakkaan, jolla on toimipisteitä kytkettynä vain yhden operaattorin virtuaaliverkkopalveluun, tulee voida luottaa, että hänen tietoturvansa ei huonone verkkojen yhteenliittämisen seurauksena.

4.4 Operaattoria koskevat tietoturvallisuuskysymykset

Tämän työn tietoturvallisuusnäkökulma on tiivistettynä: *miten suojautua toisten operaattorien verkoissa ja vastuualueella ilmeneviltä puutteilta?* Nämä puutteet saattavat olla joko puutteita tietoturvassa sinänsä taikka esimerkiksi virheellisistä konfiguraatioista aiheutuvia, tietoturvaan vaikuttavia, puutteita. Operaattorin oman toiminnan tietoturvasta huolehtiminen on tämän työn aihepiirin ulkopuolella, sen odotetaan selkeyden vuoksi olevan kunnossa. Toisten operaattorien tietoturvakäytännöistä taas ei voida olla täysin perillä, joten niitä voidaan pitää potentiaalisesti puutteellisina. Yhteenliittämisellä voi lisäksi olla vaikutuksia verkon (yhden autonomisen alueen) sisäiseen turvallisuuteen (lähinnä yhteenliittämisen ja operaattorien välisen yhteistoiminnan mahdollisesti vaatimien uusien hallintajärjestelmien ja -käytäntöjen takia).

RFC 4111:n luvussa 8 on listattu seuraavia VPN-palveluntarjoajan tietoturvaan liittyviä kysymyksiä [Fan05] (tarkempi erittely löytyy suluissa mainituista alaluvuista):

1. Runkoverkon hallintatason suojaaminen (4.4.1).
2. Runkoverkon välitystason suojaaminen (4.4.2).
3. Yhteyksien luotettava tunnistaminen runkoverkon ja asiakastoimipisteen välillä (4.4.3).
4. Reititys VPN-asiakkaiden kanssa (4.4.4).
5. Palvelun laatu asiakasliitännöissä (4.4.5).
6. VPN-asiakkaiden tietoturvan varmistaminen ja tukeminen (4.4.6).

Lisäksi *operaattorin oman verkon turvallisuuden ja strategisten tietojen omana tietona pitämisen* näkökulmasta on huomioitava:

7. Palvelun tuottamisen edellyttämä operaattorin *oman verkon strategisten tietojen paljastaminen partnerille*; (alaluku 4.4.7).
8. Useamman operaattorin kattavan *virtuaaliverkkopalvelun hallinta*, ilman että operaattoreiden tulee antaa pääsy toisilleen varsinaisiin verkon hallintajärjestelmiinsä taikka (PE-)reitittimiinsä. (4.4.8).

4.4.1 Runkoverkon hallintatason suojaaminen

Hallintatasolla (*Control Plane*) tarkoitetaan verkon ”älyä” eli tietoa siitä, miten verkon laitteiden tulee toimia. Olennaisin osa hallintatasoa on reititystiedon laskenta,

ylläpito ja vaihto muiden reititinten kanssa. Runkoverkon kontekstissa tämä reititystieto koskee eri runkoreitittimien ja niitä tukevien palvelimien[39] osoitteita ja näihin mahdollisesti johtavia leimakytkettyjä polkuja. Eli tällainen tieto on esimerkiksi missä tietty PE- tai ASBR-reititin on ja miten sinne lähetetään paketti (mutta tieto siitä, että tietyssä osoitteessa on PE- tai ASBR-reititin, välitetään osana VPN-signalointia).

Runkoverkon hallintatason suojaamisella tarkoitetaan sekä hallintason toiminnan turvaamisista että sen käsittelemän tiedon oikeellisuutta. Perinteisesti näiden on ajateltu olevan kunnossa, kun on huolehdittu hallintatiedon vaihdon kumppanin luotettavasta tunnistamisesta ja runkoverkon elementtien (käytännössä lähinnä PE-, P-reitittimien ja mahdollisen RR-reitittimen) suojaamisesta [Fan05]. RFC 3809:ssä sama asia on sanottu hieman toisin: valitun virtuaaliverkkopalvelun toteutustavan pitää pystyä suojautumaan erilaisilta hajautetuilta palvelunestohyökkäyksiltä, virhekonfiguroinneilta ja luvattomalta pääsyltä verkon hallintamekanismeihin [Nag04]. Inter-AS-tapauksessa, erityisesti kun kyseessä on useampi operaattori, tulee mukaan vielä signalointikumppanin lähettämän tiedon oikeellisuus. Tieto voi olla väärää joko virheen seurauksena tai tahallisesti (jolloin tietysti vaadittu luottamus on vaakalaudalla). Joka tapauksessa tämä ei saisi vaikuttaa operaattorin omaan tai sen asiakkaiden tietoturvaan. Edellä mainitut vaatimukset voi laajentaa koskemaan autonomisten alueiden yhteenliittämistä: *yhteenliittämistavan tietoturvaa pohdittaessa tulee ottaa huomioon suojaus palvelunestoa, virhekonfigurointeja ja luvattoman pääsyn yrityksiä vastaan. Lisäksi tulee huomioida signalointitiedon alkuperän tunnistus ja käsittely sen mukaan.*

Palvelunesto voi perustua virhetoiminnallisuuden[40] lisäksi resurssien loppumiseen. Reitittimen (ja sitä kautta verkon) hallintasolla on käytettävissään kolmea eri resurssia: laskentateho, muisti ja kommunikointikyky muiden kanssa. Reitittimen laskentateho kuluu pääasiassa reititysmuutosten vaatimaan laskentaan; sitä kuluttavat siis tiheät reititysmuutokset ja suuri (muuttuvien) reittien määrä. Reitittimen muistien kulutus on suoraan riippuvainen reittien määrästä. Kommunikointikyky muiden reititinten kanssa riippuu sekä reitityksen toimivuudesta että reitityksen käytettävissä olevasta linkkikapasiteettista. Palvelunestoa (sekä hyökkäyksistä että virhetoiminnasta johtuvia) voidaan siis estää huolehtimalla, että reititin ei saa liikaa reitityspäivityksiä eikä liikaa reittitietoa. Pitää myös huolehtia, että linkkikuorma ei pääse liian suureksi.

---

[39] Tällaisia palvelimia voivat olla esimerkiksi nimipalvelimet (DNS) ja hallintaan liittyvät palvelimet.

[40] Virhetoiminnallisuudet ovat tämän työn rajauksen ulkopuolella.

Yhteenliittämisen kannalta on oleellista miettiä, voiko reititin rajoittaa reittimainostuksien määrää jossain yhteenliittämistavassa paremmin kuin muissa ja pysyykö reittien määrä paremmin hallinnassa eri malleissa. Kommunikointikyky liittyy liikenteen välitykseen, joten se käsitellään tarkemmin myöhemmin.

#1. Voiko AS-rajan yli signaloiva reititin rajoittaa reittimainostuksien määrää?

#2. Pystytäänkö reittien määrää hallitsemaan jossain verkkoarkkitehtuurissa paremmin kuin toisissa?

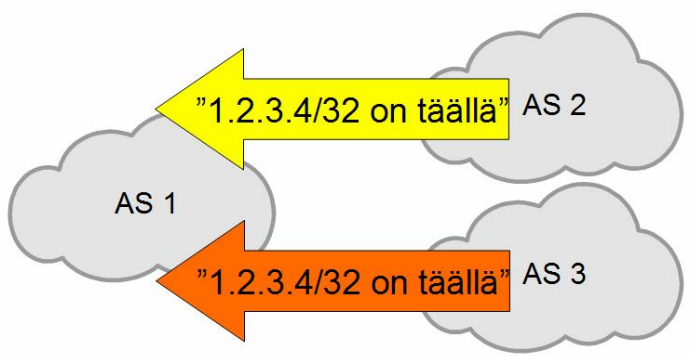
Konfigurointivirheitä voi olla monenlaisia, joten niiden kaikkien huomioiminen on mahdotonta. Virhekonfigurointeja voi olla sekä tahallisia että tahattomia. Niistä voi aiheutua toimimattomuutta tai väärää toiminnallisuutta. Virheiden tahallisuutta tai tahattomuutta on teknisesti mahdotonta erotella toisistaan; käytännössä tulee keskittyä virheiden vaikutuksen minimoimiseen ja virheiden havaitsemiseen. Lisäksi tahallisten virheiden todennäköisyyttä vähennetään määrittelemällä kenellä on konfigurointioikeudet mihinkin verkon osaan (tätä käsitellään hallintaan keskittyvässä alaluvussa 4.4.8).

Verkon, jonkin sen osan tai palvelun toimimattomuus voi riippua monesta seikasta ja sitä voi olla vaikea havaita hallintatasolla. Toimimattomuus huomataan yleensä ongelmina palvelun käytössä eli yleensä liikennöintitasolla – liikenne ei kulje. Hallintatasolta voidaan toki käynnistää esimerkiksi testi, jossa testataan ja raportoidaan tietyn palvelun toimivuus. Virtuaaliverkkoihin liittyen tällaiset testaukset tehdään tyypillisesti päästä-päähän joko PE-reititinten tai jopa toimipisteissä olevien laitteiden välillä. Tällainen testaaminen ei riipu yhteenliittämistavasta, eikä sitä niin ollen tarkastella tässä työssä.

Konfiguraatiovirheiden havaitsemisen ja niiden vaikutusten rajoittamisen keinona on määritellä, minkä tyyppisiä tietoja hyväksytään mistäkin suunnasta ja miltä kumppanilta. Tämäntyyppinen suodattaminen on normaalia BGP-reitityksessä, jossa naapurin ja reittimainostuksen tietojen (osoiteavaruus ja sen attribuutit) perusteella reittimainostuksia voidaan joko hyväksyä tai hylätä [Rek06][San06]. Myös LDP:ssä voidaan käyttää IP-osoitteisiin perustuvaa suodatusta [Cis06][Jun05b]. Tällä tavalla voidaan suodattaa esimerkiksi tiedot, joissa omassa verkossa olevan PE-reitittimen väitetään olevan naapuriverkossa. Käytännössä tämä riski on lähes olematon omien osoitteiden suhteen kahdesta syystä: ensinnäkin oma osoite näkyy verkon sisäisessä reititysprotokollassa (IGP), jota suositaan reitityspäätöksissä. Toiseksi omien

osoitteiden suodattaminen ulkoisista mainostuksista on rutiinitoimenpide, joka on suhteellisen helposti ylläpidettävä[41].

Ongelmallisempia ovat sen sijaan muiden verkkojen käytössä olevat osoitteet. Kuvassa 31 esimerkkinä kaksi eri verkkoa mainostaa samaa osoitetta AS1:lle. Osoite voisi olla PE-reitittimen osoite, sillä sen verkko-osa on 32 bittiä pitkä. Ilman tietoa eri AS:ien osoitteistuksesta ja tämän mukaan ylläpidettyjä suotimia AS1 saattaa hyväksyä kumman tahansa reitti-ilmoituksen. Lisäksi tilannetta saattavat sotkea varmistukset, joissa esimerkiksi AS2:ssa oleva osoite näkyy myös AS3:n kautta. Tämäntyyppinen tilanne tulee sitä monimutkaisemmaksi, mitä enemmän operaattoreita, niiden keskinäisiä liitäntöjä ja osoitteita on käytössä.



Kuva 31. Esimerkki konfigurointivirheestä: ristiriitaiset osoitemainostukset, joiden seurauksena PE-reititin näyttää olevan kahdessa eri verkossa

Edellä kirjoitetun olen kirjannut kriteeriksi:

#3. Onko yhteenliittämismalli altis väärille ”globaaleille” osoitemainostuksille?

Luvaton pääsy voidaan jakaa kahteen osaan: suoranaiseksi pääsyksi reitittimiin (ja muihin verkkojärjestelmiin) ja toisaalta pääsyksi reititysprosessiin. Suoranainen pääsy reitittimiin edellyttää sitä, että niihin on:

- mahdollista liikennöidä oman verkon ulkopuolelta kaksisuuntaisella yhteydellä;
- liitäntää, johon on pääsy ulkopuolelta, voidaan käyttää konfigurointiin;
- pääsyn lisäksi tulija osaa tunnistautua hyväkstyttävällä tavalla (esimerkiksi tietämällä käyttäjätunnuksen ja salasanan) tai osaa ohittaa tunnistautumisen.

Kaksisuuntainen yhteys vaatii yhteyttä hyökkääjältä hyökkäyksen kohteelle ja takaisin. Koska leimakytkentäinen verkko on pohjimmiltaan IP-verkko, jonka hallintataso

[41] Ylläpidon edellytyksenä on luonnollisesti selkeä osoitteistus ja ohjeistus, mutta ne vaaditaan kaikissa yhteenliittämismalleissa, joten niihin ei tässä paneuduta.

käyttää IP-protokollaa, on runkoverkon reitittimillä omat IP-osoitteensa, joihin on verkon toimimiseksi päästävä verkon (AS:n) sisältä. Yleensä muilla kuin toisilla runkoverkon laitteilla tai verkonhallinnan järjestelmillä ei olla yhteydessä näihin reititinten omiin osoitteisiin[42]. Toisin sanoen AS:tä ei tarvitse mainostaa reitittimien osoitteista ulospäin kuin ASBR:n peerausosoitetta. Riippuen VPN:ien tarjoavien verkkojen yhteenliittämismallista, voi olla tarvetta avata muitakin osoitteita (RR-, PE- ja VPLS-hub-reitittimet) ulkopuolisille. Muut reititinosoitteet voi jättää mainostamatta ja ne voivat olla vaikka yksityiseen käyttöön tarkoitetusta osoiteavaruudesta, jolloin niitä ei edes hyvän tavan mukaan saa mainostaa muille operaattoreille [Rek96]. Tällaisten osoitteiden käyttö on hyödyllistä erityisesti jos operaattori haluaa ”piilottaa” runkoinfrastruktuurinsa [Beh06]. Vaikka operaattori käyttäisi julkisia osoitteita reitittimiensä osoitteina, voi se jättää osoitteet mainostamatta naapureilleen. Tämä ei kuitenkaan ole yhtä tehokasta, sillä nämä osoitteet on allokoitu operaattorille julkisessa Internet-osoiterekisterissä, jota voidaan edelleen käyttää oletusreititykseen. Myöskään yksityisten osoitteiden käyttö ei ole täysin varmaa, sillä päästyään verkon sisälle yksityisiin osoitteisiin suunnatut paketit reitittyvät kuin mitkä tahansa paketit.

Osoitteilla, jota ei mainosteta reitityssanomissa verkosta ulos, on se etu, että niihin kohdistuva liikenne voidaan suodattaa automaattisesti uRPF-mekanismilla. Yksityisten alueiden osoitteilla on se lisäetu, että niihin suuntautuvat paketit suodatetaan oletusarvoisesti AS:n ulkopuolelta tulevasta liikenteestä. Myös muut runkoverkon reitittimiin suuntautuvat paketit voidaan suodattaa AS-rajalla, pois lukien edellä mainitut VPN-yhteenliittämismallin vaatimiin kohdeosoitteisiin menevät. Tästä voi tulla ylläpidollista urakkaa, kun osaan runkoverkon laitteista tulee sallia liikennöinti, osaan ei. Tästä seuraavat kriteerit:

#4. Mainostetaanko PE- ja muiden reitittimien osoitteita muihin AS:in?

#5. Täytyykö PE- ja muissa runkoverkon reitittimissä käyttää julkisia IP-osoitteita?

Vaikka AS-rajalla suodatettaisiin kaikki runkoverkon laitteisiin suuntautuva IP-liikenne[43], on niihin silti mahdollista lähettää liikennettä AS:n ulkopuolelta, jos se on tunneloitu AS-rajan yli. Tunnelointi vaatii yleensä konfiguroimista sen päätepisteissä,

---

[42] Poikkeuksena ovat luonnollisesti laitteet, joiden tehtävänä on kommunikoida ulkopuolisten verkkojen kanssa. Lisäksi verkon diagnosointiin käytettävät työkalut (kuten ping) voivat vaatia toimiakseen ulkopuolelta saavutettavissa olevat osoitteet.

[43] Runkoverkon laitteisiin suuntautuvalla liikenteellä tarkoitetaan tässä IP-paketteja, joiden otsakkeen kohdekentässä on runkoverkon laitteen IP-osoite.

mutta MPLS:n tapauksessa tuo konfigurointi on tehty, jos leimakytkettyä liikennettä hyväksytään rajan yli. Myös MPLS-VPN:issä, jotka käyttävät IP- tai GRE-tunnelointia, on tunnelin pää jo olemassa. Tästä seuraa kriteeri:

#6. Tarvitseeko verkkorajapinnan yli mainostaa leimoja, joiden leimakytketty polku päättyy johonkin runkoverkon reitittimeen tai pitääkö runkoverkon reitittimissä olla avoimia tunnelin päätepisteitä?

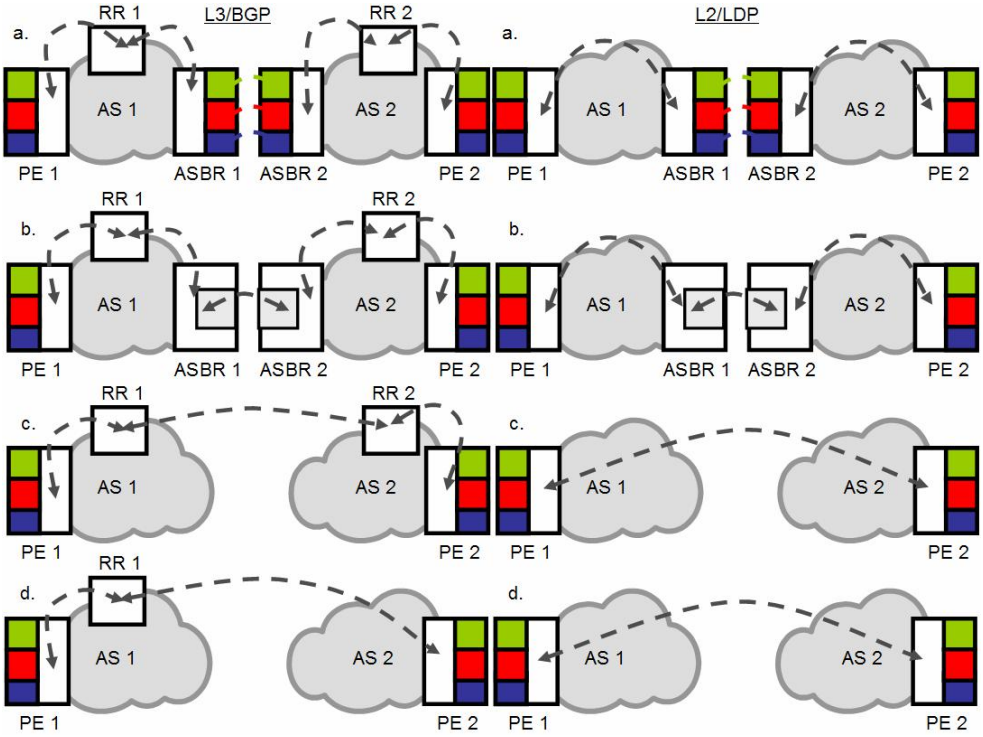
Autonomisten alueiden liittäminen tuo uudet rajapinnat ASBR-reitittimeen ja toteutustavasta riippuen mahdollisesti VPN-signaloinnin osalta PE-reitittimiin, BGP-reittiheijastimiin ja VPLS-hubeihin. Mikään yhteenliittämismalleista ei tuo käyttöön uusia protokollia, vaan yhden autonomisen alueen sisällä VPN-signalointiin käytettäviä BGP- ja LDP-protokollia voidaan käyttää myös liitettäessä autonomisia alueita yhteen. Myös mahdollisesti tarvittava leimatiedon välitys AS-rajapinnan yli hoituu BGP-protokollalla. Autonomisten alueiden välinen liikenteen hallinta on tällä hetkellä IETF:ssä kehityksen alla, eikä sen mahdollisesti tuomia uusia protokollia oteta tässä huomioon. Samoin on laita ryhmälähetyksen (multicast) osalta.

Sekä BGP:ssä että LDP:ssä signalointikumppani voidaan varmistaa käyttäen MD5-algoritmiin perustuvaa allekirjoitusta [Hef98][And01]. Tunnistusta voidaan pitää luotettavana ja toimivana, vaikka MD5-algoritmi on murrettu [Wan05] ja sen käyttöä BGP:ssä kritisoitu [Sch07]. BGP:ssä on myös muita varmistusmekanismeja kuten TTL-mekanismia hyödyntävä *Generalized TTL Security Mechanism* (GTSM [Gil04]). BGP ja LDP toimivat molemmat TCP-protokollan päällä, jota voidaan tarvittaessa ajaa erillisen varmistetun yhteyden (esimerkiksi IPsec-salatun) päällä. Menetelmiä TCP-protokollan tekemiseksi turvallisemmaksi on esitetty myös Internet-Draftissa *Improving TCP's Robustness to Blind In-Window Attacks* [Ram07]. Salauksiin perustuvissa kumppanin varmistamisissa on skaalautuvuutta rajoittavia tekijöitä: Jokainen salattu yhteys vaatii laskentakapasiteettiä reitittimeltä ja salausavainten hallinta hankaloituu signalointintiosapuolten lisääntyessä (kunkin kumppanin kanssa tarvitaan omaa avainta, jolloin avainten ylläpito, välittäminen ja vaihtaminen vaatii omat toimenpiteensä). Tästä seuraa kriteeri:

#7. Kuinka monta signalointikumppania vaaditaan per kumppani-AS?

Välittömän signalointikumppanin varmistamista ongelmallisempaa on, että varmistaminen koskee vain tätä yhteyttä ja tiedon muuttumattomuutta tällä hypyllä. Tämän takana olevia naapureita tai reititystiedon alkuperää ei voida tällä tavoin varmistaa. Kuva 32 havainnollistaa tätä. Erilaisia mekanismeja, joilla reititystiedon alkuperä ja oikeellisuus voitaisiin varmistaa BGP-kontekstissa, on ehdotettu. Näitä ovat esimerkiksi *Secure Origin BGP* (SoBGP) [Whi03] ja Secure BGP Project

[Bbn04]. Näitä ei kuitenkaan ole laajamittaisesti tuettu ainakaan tällä hetkellä. LDP:n osalta alkuperän oikeellisuuden varmistaminen on ollut esillä moniosaisten virtuaalijohtimien (*engl. multi-segment*) puitteissa [Boc06].



Kuva 32. Signaloinnin kulkuja PE-reititinten välillä

Koska reititystiedon alkuperää ei tällä hetkellä pystytä varmistamaan reitityksessä, jossa tieto kulkee välittävien laitteiden kautta, on tällä ainoa keino varmistaa sen alkuperä vaihtamalla tietoa suoraan alkuperäisen PE:n kanssa. Kriteeri on:

#8. Onko signalointikumppanina suoraan kohde-PE, vai käytetäänkö signaloinnissa välittäviä reitittimiä?

Signaloinnin alkuperätietoa voi käyttää joko sellaisenaan (esimerkiksi ei hyväksytä mitään tietoja tietyistä alkuperistä tai lisätään tiettyä alkuperää olevaan tietoon jokin lisämääre (esimerkiksi BGP-community-attribuutti)) tai yhtenä suodattamiskriteerinä muiden ohella (vain valikoituja tietoja hyväksytään tietyistä alkuperistä). Luotettavaan tunnistamiseen perustuvat alkuperätiedot kertovat alkuperän tarkasti, mutta epätarkemmat ja -luotettavammat alkuperätiedotkin ovat käyttökelpoisia. Esimerkiksi tietoa, mistä AS:sta tieto on omaan AS:ään tullut[44], on järkevä hyödyntää, vaikka tarkempi alkuperä ei olisikaan varmistettu. Mekanismit, joilla reititystiedon alkuperä

[44] Koska BGP- ja LDP-protokollat perustuvat naapuruuteen, tämä tiedetään aina.

voidaan tunnistaa luotettavasti, takaavat paremman turvan erityisesti pahantahtoista turvallisuusuhkaa vastaan, mutta ”turvattomammat” menetelmät ovat riittäviä monia tahattomien virheiden aiheuttamia tietoturvariskejä vastaan. Lisäksi ne ovat yleisesti käytettyjä BGP-ympäristössä ja siten luontevia, helpohkoja toteuttaa ja skaalautuvia.

Esimerkki edellä mainitusta on useamman kohdesuotimen käyttö VPN-reiteissä. Tällöin yhtä RT:tä voidaan käyttää ”perinteiseen tapaan” yksittäisen virtuaaliverkon topologian muodostamiseen ja yhtä tai useampaa RT:tä AS-topologian[45] muodostamiseen. LDP:ssä ei ole RT:tä vastaavaa konseptia, joten tämä kriteeri koskee vain BGP:llä signaloituja VPN-palveluita:

#9. Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?

4.4.2 Runkoverkon välitystason suojaaminen

Runkoverkon välitystason suojaamisella tarkoitetaan sitä, että välitettävä liikenne ei pääse muuttumaan matkalla. Normaalisti tämän oletetaan olevan kunnossa yhden operaattorin verkon sisällä (fyysinen suojaus). Jos on syytä epäillä, ettei fyysinen suojaus ole kunnossa, voidaan käyttää salausta reitittimien välisillä yhteyksillä (esimerkiksi PE-reititinten välinen liikenne voisi olla salattu) [Beh06]. Myös yksittäisiä linkkejä voidaan suojata (erityisesti tämä koskee kahden eri AS:ssä olevan ASBR:n välistä yhteyttä, jos se on toteutettu ei-luotetun yhteyden yli esimerkiksi yleisessä Internet-yhteyden jakopaikassa[46], CIX:issä). Tästä seuraavat kriteerit:

#10. Voidaanko rajareititinten välisellä yhteydellä käyttää IPsec:iä?

#11. Voidaanko PE-PE-väleillä käyttää IPsec:iä?

Paitsi pakettien sisällön muuttumattomuus runkoverkossa, olennaista on myös ylipäänsä runkoverkon kyky välittää paketteja. Tähän vaikuttaa paitsi aiemmin käsitelty reititys, myös linkkikuormitus. Operaattorit pyrkivät takaamaan asiakkaiden palvelutason varaamalla riittävästi kapasiteettia yhteyksilleen reitittimien välille. Sekä linkkikapasiteetin käytön tehostamiseksi että kaupallisista syistä useat operaattorit

[45] AS-topologia muodostavat ne AS:t, joihin tietyn VPN:n toimipisteet ovat liitettyinä – lisättyinä tarvittavilla transit-AS:illä.

[46] Yleistä Internet-liikenteen vaihtopaikkaa kehotetaan välttämään MPLS-VPN:ien yhteenliittämispaikkana ohjeistuksissa paitsi tietoturvallisuuden, niin myös palvelun laadun näkökulmasta [Beh06].

käyttävät laatuluokitusta. Käytetyistä liikenneluokista ja halutusta palvelutasosta riippuen operaattoreilla on erilaisia sääntöjä siitä kuinka paljon minkäkin liikenneluokan liikennettä saa kullakin linkillä olla. Säännöt ohjaavat linkkien päivityksiä (yleensä nopeuden nostoja) yhdessä mittaustiedon ja ennustusten kanssa. Toisaalta valittu QoS-politiikka ohjaa asiakkaiden kanssa tehtäviä sopimuksia ja niiden noudattamista (esimerkiksi liikenteen rajoitus sovittuihin kapasiteetteihin). Yleensä pyritään siihen, että muuta kuin best-effort-liikennettä rajoitetaan vain suoraan asiakasyhteyksillä[47], eikä korkeamman laatuluokan liikennettä pudoteta tai tarpeettomasti jonoteta muualla. AS:iä yhteenliitettäessä haasteena on, että rajareititinten välinen liitäntä on runkoliitäntä (tai monta asiakaskohteista liitäntää riippuen inter-AS-mallista), mutta tulee oman hallinnan ulkopuolelta. QoS-mallin toiminnan kannalta oleellista on ennustettavuus, joka yleensä varmistetaan muun muassa rajoittamalla ulkoa tuleva liitäntä tietyn liikenneprofiilin mukaan. Puhtaasti oman verkon QoS:n toimivuuden kannalta rajoittaminen on mahdollista tehdä rajareititinten väliselle liitännälle, mutta riippuen valitusta yhteenliittämistavasta, se voi kohdistua satunnaisesti asiakkaiden liikenteeseen. Liikenteen rajoittaminen kun yleensä perustuu paketin liikenneluokkaan ja runkoverkossa kaikkien asiakkaiden liikenteet menevät samoihin liikenneluokkiin[48]. Kriteeri:

#12. Voidaanko rajareitittimessä tehdä asiakaskohtaista liikenteenrajoitusta?

4.4.2.1 Mahdollisuus suodattaa leimattua liikennettä verkkorajapinnoissa

Eräs pakettiverkkojen tietoturvan varmistava toimenpide on mahdollisuus suodattaa verkkoon tulevaa liikennettä. Operaattori voi jättää välittämättä paketit, jotka eivät suuntaudu esimerkiksi operaattorin itsensä tai operaattorin asiakkaan käytössä oleviin järjestelmiin. Operaattori voi myös suodattaa paketit, jotka suuntautuvat esimerkiksi verkonhallinnan järjestelmiin, mutta joihin ei tule päästä operaattorin oman verkon ulkopuolelta. Operaattori voi lisäksi suodattaa tilapäisesti paketit, jotka ovat menossa sinänsä oikeisiin kohteisiin, mutta joiden epäillään olevan haitallista liikennettä[49]. IP-verkoissa tämä suodattaminen perustuu yleisesti lähde- ja kohdeosoitteisiin ja lisäksi mahdollisesti joihinkin muihin tietoihin ja määreisiin[50].

---

[47] Tämä tarkoittaa PE:n asiakkaaseen päin olevaa liityntää tai CE:n PE:hen päin osoittavaa liityntää.

[48] Teoriassa pienelle määrälle asiakkaita voisi tehdä omia laatuluokkiaan, mutta tämän ratkaisun skaalautuvuus on erittäin huono.

[49] Tällainen tilanne voisi olla esimerkiksi operaattorin havaitsema palvelun esto –hyökkäys.

[50] Näitä lisämääreitä ovat esimerkiksi protokollat ja protokollien porttinumerot.

Tässä työssä käsitelty MPLS-leimoilla varustettu liikenne on IP-liikennettä monimutkaisempaa suodattaa monestakin syystä:

- MPLS-leimat ovat ”vain numeroita”; ne eivät sisällä osoiteinformaatiota, eivätkä tietoa kontekstista, jossa niitä on tarkoitus käyttää [Ros01a].
- Leimojen myöntäminen ja jako on verkossa hajautettu prosessi. Vain *leiman myöntäjä* R_d ja *leimatiedon vastaanottaja* R_u tietävät leiman merkityksen. Hajautuksesta johtuen samaa leimaa (saman numeroarvoista) voidaan myös käyttää eri puolilla verkkoa eri tarkoituksissa [Ros01a].
- Paketissa voi olla useampi leima ”pinossa” [Ros01a].
- MPLS-leimat eivät sisällä tietoa, kuka on liittänyt ne pakettiin [Ros01a].
- Välitettävät paketit eivät välttämättä sisällä IP-otsakkeita lainkaan, jolloin niistä ei luonnollisesti löydy myöskään IP-osoitteita, joiden perusteella suodatusta olisi mahdollista tehdä. Tällainen tilanne voi olla kuljetettaessa linkkikerroksen liikennettä MPLS-verkon yli [Mar06c].
- Vaikka leimattu paketti sisältäisi IP-otsakkeen, ei IP-osoitetietoa ole välttämättä mielekästä käyttää suodattamiseen. Erityisesti näin on VPN-liikenteen kohdalla, jolla on runkoverkoista (Internetistä) riippumaton osoitteistus ja reititys [Ros06a]. Tällöin IP-osoite ei kerro liikenteen lähdettä eikä kohdetta runkoverkon kontekstissa. Koska MPLS-leimatussa paketissa mikään ei suoranaisesti kerro, onko paketin sisältö VPN-liikennettä vai ei, ei leimattujen pakettien IP-osoitteita voi käyttää liikenteen suodattamiseen linkillä, jossa voidaan välittää myös VPN-liikennettä.

Edellä mainituista syistä johtuen *leimakytkevä reititin voi suodattaa leimattua liikennettä ensisijaisesti leimojen perusteella*. Tämä pätee erityisesti toiseen operaattoriin suoraan liittyvään ASBR-reitittimeen. Toisaalta: *suodattaakseen liikennettä leimojen perusteella, ASBR-reitittimen pitää tietää leimojen merkitys*. Yksinkertaisin tapa on, että ASBR on itse kaikkien niiden leimojen myöntäjä, joita toisesta verkosta tulevissa paketeissa saa olla. Muussa tapauksessa ASBR:n pitää saada tietoonsa ”sallitut leimat” jollain muulla tavalla. Näitä tapoja ei toistaiseksi ole standardoitu [Ros06a].

Olen muokannut edellä mainituista vaatimuksista kriteerin:

#13. Voidakseen suodattaa leimattua liikennettä verkkorajapinnassa, ASBR:n pitää itse olla niiden leimojen myöntäjä, jotka toisesta verkosta tulevien pakettien leimapinoissa saa olla.

4.4.3 Linkkien autentikointi runkoverkon ja asiakastoimipisteen välillä

Inter-AS ei vaikuta asiakasyhteyksiin. Verkkojen yhteenliittämistä käsiteltäessä voisi ajatella asiakasyhteyden sijasta tarkasteltavan rajareititinten välistä yhteyttä. Se on käsitelty kriteerin #10 kohdalla, joten en tee siitä omaa kriteeriään.

4.4.4 Reititys VPN-asiakkaiden kanssa

Inter-AS ei vaikuta asiakasyhteyksiin. Verkkojen yhteenliittämistä käsiteltäessä voisi ajatella asiakasyhteyden sijasta tarkasteltavan verkkojen välistä reititystä. Autonomisten alueiden välinen reititys on vertailtavissa malleissa keskeinen komponentti ja sitä on vertailtu eri kohdissa, joten en tee siitä omaa kriteeriä.

4.4.5 Palvelun laatu asiakasliitännöissä

Inter-AS ei vaikuta asiakasyhteyksiin. Verkkojen yhteenliittämistä käsiteltäessä voisi ajatella asiakasyhteyden sijasta tarkasteltavan verkkojen välistä palvelun laatua rajareititinten välisellä yhteydellä. Tämä on käsitelty jo kriteerin #12 kohdalla, joten en tee tästä erillistä kriteeriä.

4.4.6 VPN-asiakkaiden tietoturvan varmistaminen ja tukeminen

Asiakkaiden tietoturvan varmistaminen käsitellään asiakasvaatimusten yhteydessä alaluvussa 4.5.

4.4.7 Operaattorin verkon strategisten tietojen pitäminen salassa

Operaattori saattaa haluta pitää oman *runkoverkkonsa topologian salassa* sekä *tietoturvallisuus- että strategisista syistä*. Runkoverkon topologian tunteminen saattaa heikentää verkon tietoturvallisuutta helpottamalla verkon toiminnan sabotoimista joko reitittinten heikkouksia hyödyntämällä, sopivasti kohdistetulla haitallisella verkkoliikenteellä (palvelunestohyökkäys) tai fyysisesti verkkoa vahingoittamalla. Strategisista syistä taas ei välttämättä haluta kertoa muille operaattoreille esimerkiksi omien reitittinten lukumäärää, kokoa taikka sijainteja.

Operaattoreiden välillä tietoa liikkuu sekä automaattisesti verkon toiminnan yhteydessä että verkon ulkopuolella. Verkon ulkopuolella, kuten operaattorien välisissä neuvotteluissa ja sopimuksissa, operaattorit joutuvat paljastamaan verkoistaan erinäisiä tietoja, jotta voivat suunnitella ja toteuttaa yhteiseksi aiottua palvelua. Tällaisia tietoja ovat esimerkiksi verkon maantieteellinen kattavuus, tähän mahdollisesti liittyvä aikataulu ja verkossa noudatettava QoS-malli. Kuinka paljon ja minkälaisia tietoja operaattorit luovuttavat toisilleen, riippuu luonnollisesti palvelusta, jota ne yhdessä aikovat tuottaa, ja kumppanuuden asteesta[51]. Verkoissa itsessään automaattisesti liikkuva tieto tarkoittaa tässä yhteydessä erilaisten reititysprotokollien mukanaan kuljettamaa tietoa. Tässä alaluvussa keskitytään näihin automaattisesti liikkuviin tietoihin, koska verkon ulkopuolella liikkuvat tiedot eivät suoranaisesti riipu tavasta, jolla verkot liitetään toisiinsa.

Leimakytketyissä verkoissa reititystietoa on tarve välittää vain niistä osoitteista, joihin liikennöidään tai joita käytetään leimakytkettyjen polkujen päätepisteinä[52]. Reitittimien osoitteita tulee välittää vain niissä tapauksissa, joissa reitittimiin on tarkoitus päättää leimakytkettyjä polkuja tai joissa on tarvetta kommunikoida itse reitittimen kanssa[53]. ASBR-reititinten, joiden tehtävä on kommunikoida toisen verkon kanssa, lisäksi verkkorajapinnan yli täytyy välittää tietoja korkeintaan niistä PE-reitittimistä, joissa on inter-AS-asiakkaita. Seuraavaksi käyn läpi tilanteet, joissa näiden reitittinten osoitteista on tarvetta välittää tietoa verkkorajan yli.

---

[51] Kumppanuuden asteella tarkoitan tässä sitä, kuinka yhtenäiseksi operaattorit haluavat tuotantonsa.

[52] Leimakytketyn polun päätepiste ei välttämättä ole liikenteen kohde johtuen leimapolkujen hierarkkisuudesta ja toisaalta liikenteestä, jonka kohde on leimakytketyn verkon ulkopuolella.

[53] Tällaisia tarpeita ovat lähinnä verkonhallinnan tarpeet ja signaloiti- ja reititysprotokollat.

Reitityksen näkökulmasta leimakytkentää hyödyntävillä virtuaaliverkkopalveluilla on kaksi vaatimusta:

- PE-laitteen on kyettävä kytkemään runkoverkosta tulevat paketit oikeaan, tiettyyn virtuaaliverkkoon liitettyyn, toimipisteeseen virtuaaliverkkoleiman perusteella (ja vastaavasti lisäämään tietystä toimipisteestä tulevaan pakettiin tätä vastaava virtuaaliverkkoleima).
- Virtuaaliverkkoleimoilla leimatun liikenteen välittämiseksi PE-laitteiden, joissa on kyseisen virtuaaliverkon toimipisteitä kytkettyinä, välillä on oltava kuljetustunneli.

Ensimmäinen näistä vaatimuksista tarkoittaa, että on oltava *mekanismi, jolla PE-reitittimet saavat vaihdettua tiedon VPN-leimoista*. Eri VPN-palveluissa tämä tiedonvaihto tehdään eri tavoin. RFC4364:n mukaisissa L3-VPN:issä ja RFC 4761:n mukaisissa VPLS:issä tiedonvaihtoon käytetään BGP-protokollaa ja muissa tässä työssä käsitellyissä LDP-protokollaa. BGP:ssä on luontaisesti olemassa mekanismit, joilla tietoa kuljetetaan hypyin[54]. Kohdistettussa LDP:ssä ei ole määriteltynä mitään vastaavia toiminteita. Edellä mainittu tarkoittaa, että VPN-toiminnan vaatima VPN-leimojen levittäminen onnistuu BGP:ssä ilman itse PE-osoitteiden paljastamista (joko rajareititin tai reittiheijastin hoitavat signaloinnin toiseen verkkoon). Sen sijaan LDP:tä käytettäessä tämä ei ole mahdollista[55].

Itse VPN-leimojen levittämismekanismin lisäksi myös signaloinnin sisällössä kuljetetaan PE-reititinten osoitteita, koska nämä ovat kuljetustunneleiden päätepisteitä. Siis, vaikka VPN-signaloinnissa voitaisiin käyttää välittäviä reitittimiä, jolloin PE-reititinten osoitteita ei tarvitsisi paljastaa, ne paljastuvat kuitenkin kuljetustunnelien takia. Tämä on mahdollista välttää vain, jos kuljetustunneli on pätkitty eri AS-alueilla olevien PE-reititinten välillä. Tämä pätee erityisesti LDP-signaloituihin VPN:iin, sillä niissä VPN-signalointi on sidottu kiinteämmin kuljetustunnelin päätepisteisiin: PE-osoitteet voi jättää mainostamatta toiseen verkkoon vain jos kuljetustunneli on pätkitty. Tässä päädytään jo aiemmin mainittuun kriteeriin (#4):

#14. Mainostetaanko PE- ja muiden reitittimien osoitteita muihin AS:in?

[54] Tällaisia ovat jako sisäiseen ja ulkoiseen BGP:hen (iBGP ja eBGP) ja lisäksi esimerkiksi route reflector –tekniikka.

[55] LDP:tä käytettäessä signaloivat reitittimet ovat myös kytkentäpisteitä: ”hyppiminen” tarkoittaa käytännössä myös kuljetustunnelin pätkimistä.

4.4.8 Yhteisen virtuaaliverkkopalvelun hallinta erotettuna yleisestä verkonhallinnasta

Virtuaaliverkkopalvelun pystyttäminen, virtuaaliverkon lisääminen ja toimipisteiden lisääminen vaatii konfigurointia ainakin PE-reitittimiin, joihin toimipisteet liitetään liitäntäpiireillä. Lisäksi – riippuen yhteenliitämisen toteutustavasta – saatetaan joutua tekemään konfiguraatioita myös ASBR-reitittimiin, H-VPLS-verkon hubeihin ja RR-reitittimiin. Vastaavasti purettaessa virtuaaliverkkoa tai sen topologiaa muutettaessa (lisättäessä tai poistettaessa toimipisteitä, lisättäessä varmistavia yhteyksiä, vaihdettaessa QoS-parametreja, jne.) pitää tehdä konfiguraatiomuutoksia reitittimiin. Myös liikennetiedon keräys ja vianselvitys saattaa vaatia pääsyä reitittimiin. Konfiguraatioita voidaan tehdä joko suoraan reitittimiin taikka jonkin hallintajärjestelmän kautta. Reitittimissä erilaisten käyttäjäprofiilien tuki on hyvin vaihtelevaa; yleisesti ottaen on joko oikeus tehdä konfiguraatiomuutoksia tai sitten pelkästään lukea konfiguraatioita ja laskureita: välimuotoja ei ole (poikkeuksena lähinnä erilaiset virtuaalireititintyyppiset toteutukset, jotka eivät sovi tähän). Tietoturvasyistä ulkopuolisille operaattoreille ei haluta antaa täysiä lukuoikeuksia omiin reitittimiin, puhumattakaan vapaan konfiguroinnin mahdollisuudesta. *Käytännössä tämä tarkoittaa erillisen järjestelmän käyttämistä*, jonka kautta ulkoisen operaattorin henkilökunta pääsee käsiksi liikennedataan ja tekemään tarvittavia konfiguraatioita ilman suoraa pääsyä reitittimiin. Tämän *lisäksi viankorjausprosessiin tulee kiinnittää erityistä huomiota, jotta kunkin eri operaattorin verkonhallinta- ja viankorjaushenkilöstö osaa toimia ongelmatilanteissa kitkattomasti yhdessä*.

Yhteenliittämistapa erottaa hallinnan mahdollisuuksia ainostaan transit-operaattorin tapauksessa, jolla ei ole lainkaan PE-reitittimiä. Toisissa yhteenliittämistavoissa täytyy tehdä asiakaskohtaisia konfiguraatiota rajareititimiin, toisissa ei. Tästä seuraa vertailukriteeri:

#15. Vain PE-reitittimiin on tehtävä asiakaskohtaisia määrityksiä

4.5 Virtuaaliverkkopalvelun asiakasta koskevat tietoturvallisuuskysymykset

Virtuaaliverkkopalvelun käyttäjät odottavat palvelulta turvallista ja yksityisyyden säilyttävää toimintaa. Asiat, joita virtuaaliverkkopalvelun käyttäjät voivat palvelultaan odottaa, ja jotka operaattorin pitää pystyä takaamaan, on lueteltu RFC 4111:n luvussa 7 (tarkempi erittely löytyy suluissa mainituista alaluvuista):

1 Erillisyys (alaluku 4.5.1)

2 Suoja (4.5.2)

3 Yksityisyys (Confidentiality) (4.5.3)

4 CE-laitteen luotettava tunnistaminen (4.5.4)

5 Eheys (Integrity) (4.5.5)

6 VPN-liikenteen uusiokäyttö haitallisessa tarkoituksessa (Anti-replay) (4.5.6)

Virtuaaliverkkopalveluissa on syytä erottaa toisistaan kaksi erityyppistä asiakastapausta: tilanne, jossa virtuaaliverkolla on toimipisteitä kytkettyinä useammassa autonomisessa alueessa oleviin PE-reitittimiin (ns. *inter-AS-VPN*) sekä virtuaaliverkot, joiden kaikki toimipisteet ovat kytkettyinä saman autonomisen alueen PE-reitittimiin (ns. *intra-AS-VPN*). Inter-AS-VPN:ien käyttäjien tulisi olla tietoisia riskistä, joka liittyy useamman verkon ja operaattorin käyttöön. Intra-AS-VPN:ien käyttäjien tulee voida luottaa oman palvelunsa tietoturvallisuuteen samoin riippumatta siitä, tarjoaako sen operaattori muille asiakkaille inter-AS-VPN-palvelua.

4.5.1 Virtuaaliverkon erillisyys muista virtuaaliverkoista ja julkisista verkoista

4.5.1.1 VPN-asiakkaiden osoitteistuksen erillisyys

VPN-palveluiden tulee taata, että niiden asiakkaat voivat käyttää kaikkia mahdollisia osoitteita riippumatta muiden asiakkaiden tai esimerkiksi Internetin osoitteistuksesta. Käytännössä tämä toteutuu reitityksen ja liikenteen erillisyydellä, joita käsitellään seuraavissa alaluvuissa.

4.5.1.2 Reitityksen erillisyys

Tässä työssä käsitellyistä virtuaaliverkkopalveluista vain *BGP-protokollaa ja leimakytkentää hyödyntävä IP-virtuaaliverkkopalvelu* [Ros06a] tarjoaa reititystä. RFC 4111 määrittelee reitityksen erillisyyden: ”*reititystieto ei saa vuotaa luottamusalueelta toiselle kuin erikseen niin haluttaessa* [Fan05]”. Vaikka RFC 4111 määritteleekin kaikki runkoverkko-operaattorit kuuluviksi samaan

luottamusalueeseen, voisi inter-AS-tapauksessa määritellä, että edellisen ehdon lisäksi reititystieto ei saa kulkeutua AS:stä toiseen kuin erikseen haluttaessa.

VPN-palvelun erillisyys yleisestä IP-reitityksestä perustuu erilliseen osoiteperheeseen BGP-reitityksessä. Eri VPN:ien reititystiedon erottaminen puolestaan perustuu eri reittierotin (Route Distinguisher) –arvoihin. Reititystiedon vuodattamisen hallinta puolestaan perustuu kohde-erotin (Route Target) –arvoihin. RD- ja RT-arvot ovat operaattorin kullekin VPN:lle allokoimia. Kuten kappaleessa 2.4.3 on kuvattu, sekä RD- että RT-arvot koostuvat kahdesta osasta, joista toinen perustuu joko operaattorille allokoituun AS-numeroon tai johonkin operaattorille allokoituun IP-numeroon ja toinen osa on operaattorin itse antama. Nämä kaksi seikkaa takaavat ko. osoitteiden yksilöllisyyden – edellyttäen että konfiguraatiot on tehty oikein. Malli ei kuitenkaan ota mitenkään kantaa reititysinformaation vuodattamiseen eri AS:ien välillä. Tätä varten *BGP/MPLS IP-VPN:iin* on kehitetty laajennus ”Rajoitettu BGP/MPLS IP-VPN-reittien mainostus” (suomennos omani), jossa kukin AS voi mainostaa, mitä RT-arvoja sisältäviä VPN-reittejä ne haluavat vastaanottaa. Tämä toimintamalli perustuu operaattoreiden väliselle luottamukselle, eikä sitä ole suunniteltu tietoturvaominaisuudeksi [Mar06b]. Kriteeri:

#16. Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?

4.5.1.3 Virtuaaliverkon eristäminen liikenteellisesti

Virtuaaliverkkopalvelussa halutaan eristää virtuaaliverkko muusta verkosta niin, että sen *toimipisteistä tuleva liikenne ei päädy tahattomasti*[56] *virtuaaliverkon ulkopuolelle* ja että sen *ulkopuolelta tuleva liikenne ei pääse hallitsemattomasti virtuaaliverkkoon* kuuluviin toimipisteisiin. Kommunikointiin virtuaaliverkon ulkopuolelta vaaditaan molemmat liikennesuunnat yhtä aikaa, mutta toisenkin suunnan ”vuoto” voi olla haitallinen tietoturvalle[57] ja lisäksi altistaa palvelunestohyökkäyksille. Teknisesti eri liikennesuunnat ovat erillisiä johtuen käytettyjen protokollien luonteesta, joten niitä on mielekästä tarkastella erikseen.

Hallitsematonta liikennettä virtuaaliverkosta ulos voi päästä vain jos virtuaaliverkkoon on *liitettynä asiattomia toimipisteitä*[58]. Liikennettä virtuaaliverkkoon sen ulkopuolelta

---

[56] Hallitut yhdyskäytävät virtuaaliverkon ulkopuolelle (esim. Internetiin) ovat yleisin esimerkki tällaisesta poikkeuksesta.

[57] Jopa yksittäisen paketin avulla on levitetty verkkomatoja. [Beh05]

[58] Lisäksi laitevioista johtuen liikenne saattaa päästä väärään paikkaan, mutta sitä ei tässä käsitellä.

voi päästä väärien toimipisteiden lisäksi myös, jos jokin laite leimakytketyssä verkossa käyttää tietyllä lailla virheellisiä tai *luvattomia leimoja*.

Asiattomat toimipisteet virtuaaliverkossa

Toimipisteiden liittäminen virtuaaliverkkoon tehdään hallintatasolla: *paikallisesti PE-laitteiden konfiguraatioissa*, joissa tietty liityntä assosioidaan kuuluvaksi tiettyyn virtuaaliverkkoon, ja *etätoimipisteiden*[59] *osalta joko VPN-autodiscoveryn tai paikallisen konfiguroinnin avulla*. Tämä konfigurointi tehdään erikseen jokaisessa PE-reitittimessä[60], joihin asiakkaita halutaan liittää. Näin ollen virheelliset toimipisteet virtuaaliverkossa johtuvat joko:

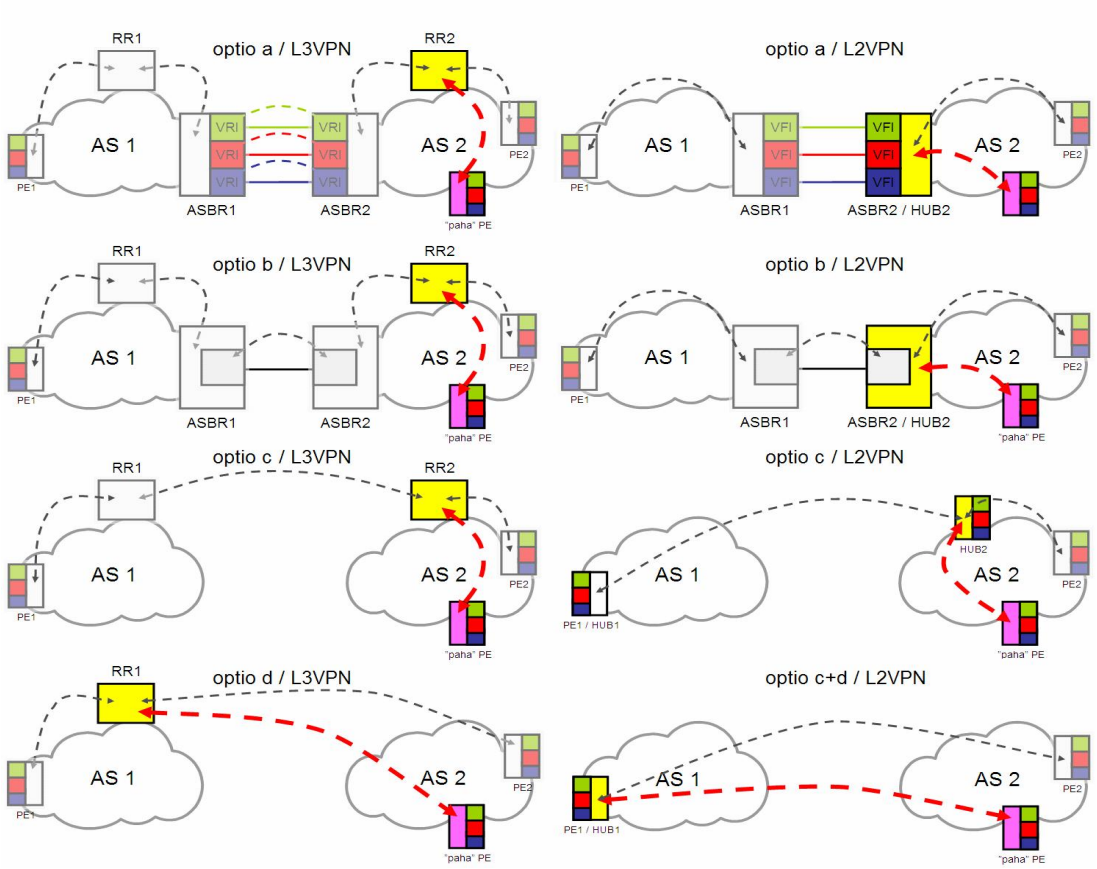
- *konfigurointivirheistä* (tahallisista tai tahattomista) PE-reitittimissä tai muissa VPN-signalointia käsittelevissä solmupisteissä (riippuen VPN-palvelusta ja yhteenliittämistavasta näitä ovat: RR:t, H-VPLS hubit, PW S-PE:t ja ASBR-reitittimet);
- *ongelmista signalointiprosessissa* (protokollan virheellisestä toiminnasta tai ei-halutuista toimijoista signaloinnissa); tai
- suoranaisista *laitevioista*.

Kuvassa 33 on esitettynä autonomisten alueiden välinen VPN-signalointi eri yhteenlittämistavoilla ja eri VPN-palveluilla. Kummassakin verkossa (AS1 ja AS2) on yksi ”laillinen” PE-reititin per AS. AS2:ssa on lisäksi asiaton laite (violetti ”paha PE”). Katkoviivat esittävät VPN-signalointiyhteyksiä. Kuva havainnollistaa, kuinka asiaton laite voi liittyä VPN-signalointiin mahdollistaen asiattomien toimipisteiden lisäämisen eri virtuaaliverkkoihin. Paksu punainen katkoviiva esittää VPN-signalointiyhteyttä, jolla ”paha PE” liittyy tapauksesta riippuen joko toiseen PE:hen, H-VPLS-hubiin taikka ASBR:ään. Yhteyden vastapää on väritetty keltaisella. Kun AS1 on oma verkko ja AS2 yhteistyökumppanin verkko, huomataan selkeästi milloin ”pahan” PE:n liittäminen voi tapahtua omalle verkolle näkymättömästi (keltainen laite AS2:ssa) ja missä tämä on omassa hallinnassa (keltainen laite AS1:ssä). Tästä seuraa vertailukriteeri:

#17. Onko signalointikumppanina suoraan kohde-PE, vai käytetäänkö signaloinnissa välittäviä reitittimiä?

[59] Etätoimipisteillä tarkoitetaan tässä yhteydessä toisiin PE-reitittimiin liitettyjä VPN-toimipisteitä.

[60] Provisionti voidaan tehdä keskitetysti jollain järjestelmällä, mutta laitetasolla se tehdään silti paikallisesti jokaisessa PE:ssä.



Kuva 33. Asiattoman PE:n lisääminen VPN-signalointiin

Kuvasta 33 näkee myös, missä tapauksissa tieto alkuperäisestä PE-reitittimestä säilyy, jolloin sen perusteella voi tehdä suodatusta (tieto säilyy niissä tapauksissa, joissa se ei käy minkään signalointia aggregoivan laitteen kautta – RR ei ole tässä mielessä aggregaattori, sillä se säilyttää alkuperätiedon). Kriteeri:

#18. VPN-reittien alkuperän säilyminen signaloinnissa

L3-VPN:ssä ja BGP:hen perustuvassa VPLS-palvelussa käytetään Route Target -attribuuttia reititystietojen suodattamiseen PE-reitittimissä VPN-topologioiden muodostamisessa. Tätä samaa ominaisuutta voidaan hyödyntää myös AS-rajalla lisäämään tietoturvallisuutta. Tämä tapahtuu esimerkiksi lisäämällä inter-AS-reitteihin ylimääräinen inter-AS-RT, jota ilman reittiä ei hyväksytä toisesta verkosta. Tämä suojaa lähinnä vahingossa tapahtuvilta virhekonfiguroinneilta (verrattuna tilanteeseen, jossa suodatus perustuu pelkästään yksittäisten RT-arvojen mukaan suodattamiseen). RT-tiedon säilyminen edellyttää MP-BGP-protokollan käyttöä. Kriteeri:

#19. Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?

Luvattomalla leimapinolla varustettu liikenne

Luvattomat leimat tarkoittavat signaloituja leimoja, joita käyttää väärä taho. Jos esimerkiksi reitittimissä PE1 ja PE2 on suoraan kytkettyinä virtuaaliverkon VPN-toimipisteitä, PE1 signaloi PE2:lle, että tämän tulee käyttää VPN-a:han tuleviin paketteihin VPN-leimaa *a*. Jos jokin muu reititin kuin PE2 lähettää PE1:teen päättyvään kuljetustunneliin paketin, jonka sisin leima on *a*, tulkitsee PE1 sen VPN-leimaksi, jolla paketti päätyy VRI-a:han ja sitä kautta edelleen VPN-a:n kuuluvaan toimipisteeseen. PE1:llä ei ole keinoa todeta, että paketti tulisi väärältä PE:ltä, koska leimoissa ei ole niiden alkuperästä kertovaa tietoa. Jos halutaan vakuuttua paketin alkuperästä, on käytettävä lisätoimenpiteitä, esimerkiksi IPsec-tunneleita [Ros06a].

Tämän työn oletuksena on, että yhden operaattorin alueella kaikki leimakytkentäiset reitittimet ovat luotettuja, mutta verkkoja yhdistettäessä näin ei ole. Toisin sanoen, pohdittavaksi jää *verkkorajapinnan yli tulevien pakettien leimojen luvallisuus.* ASBR-reititin on yhteenliittämismallista riippuen toiminnaltaan lähempänä PE-reititintä tai P-reititintä. PE-reititimet ovat määritelmällisesti LER:iä (lukuunottamatta CsC:tä), jolloin niillä on koko leimapino hallussaan, P-reittimet tyypillisesti ovat tietoisiä vain päällimmäisestä leimasta[61], eivät mahdollisista VPN-leimoista. Leimojen erilainen rooli (tunnelointileima ja VPN-leima) lisää vielä oman kompleksisuutensa asiaan.

- Laillisten leimojen laiton käyttö on mahdoton huomata AS-rajalla, mutta tässä palataan siihen, että inter-AS-asiakkaan on pakko luottaa kaikkiin palvelun tuottaviin operaattoreihin. Joka tapauksessa asiakas voi käyttää IPseciä tai muuta todennuskeinoa toimipisteiden välillä operaattoreista riippumatta.
- Koska MPLS-verkoissa LSR voi yleensä varmasti tietää vain edellisen LSR:n, josta paketti on sille tullut, ei sitä, mistä tämä on paketin saanut, merkitsee tämä käytännössä, että AS-rajalla olevan ASBR-reitittimen olisi kyettävä hallitsemaan sisääntulevien pakettien leimapinot. Toisin sanoen sen
  - olisi kyettävä lukemaan koko leimapino;
  - ymmärrettävä kaikkien leimojen merkitys kontekstissaan (tarkoittaa tässä lähinnä VPN-leimojen merkitystä).
    - Tästä seuraa, että ASBR:n olisi hyvä osallistua, tai olla ainakin tietoinen VPN-signaloinnin sisällöstä AS:ien välillä.

Kriteeri:

---

[61] Joissain liikenteenhallintatilanteissa (esim. TE-FRR) P-reitittimillä voi olla tietoa useammasta leimasta pinossa, mutta tämä on erikoistapaus, eikä liity käsiteltävään asiaan.

#20. Voidakseen suodattaa leimattua liikennettä verkkorajapinnassa, ASBR:n pitää itse olla niiden leimojen myöntäjä, jotka toisesta verkosta tulevien pakettien leimapinoissa saa olla.

4.5.2 Suoja

RFC 4111 listaa käsitteen suoja alle suojautumisen murtautumisilta, palvelunestohyökkäyksiltä ja lähdetietojen väärentämiseltä (”*spoofing*”). Suoja murtautumista vastaan käsiteltiin jo eristys-alaluvussa (4.5.1). Palvelunestohyökkäykset käsiteltiin runkoverkon osalta, mutta on joitakin yksittäisiin virtuaaliverkkoihin kohdistuvia tilanteita, jotka käsitellään seuraavassa alaluvussa (4.5.2.1). Suojautumista lähdetietojen väärentämistä vastaan käsitellään alaluvussa 4.5.2.2.

4.5.2.1 Yksittäiseen virtuaaliverkkoon kohdistuvalta palvelunestohyökkäykseltä suojautuminen

Runkoverkkoon kohdistuvat palvelunestohyökkäykset voivat aiheuttaa välillisesti palvelunestoa myös virtuaaliverkkoihin. Nämä on käsitelty luvuissa 4.4.1 ja 4.4.2. Palvelunesto voi kohdistua myös yksittäiseen virtuaaliverkkoon, vaikka runkoverkon palvelussa ei olisikaan ongelmaa. Palvelunestohyökkäys voi tapahtua sekä liikennetasolla että hallintatasolla.

Liikennetasolla virtuaaliverkossa palveluntasosta pyritään huolehtimaan oikein mitoitetuilla liitännöillä kuhunkin toimipisteeseen ja näihin liitäntöihin mahdollisesti liitetyillä palveluprofiilien mukaisilla liikenteen rajoituksilla. Yhteenliittäminen tuo kaksi uutta kysymystä: ensinnäkin toimivatko toisten operaattoreiden (PE-reititinten) hallussa olevat liikenteen rajoitukset halutusti ja toiseksi voiko virtuaaliverkkoon lähettää ulkopuolista liikennettä? Toisten osapuolten tekemät konfiguroinnit PE-reitittimissä eivät liity yhteenliittämistapaan ja ovat siten tämän työn aihepiirin ulkopuolella. Ulkopuolisen liikenteen osalta asia on taas käsitelty jo alaluvussa 4.5.1.3.

Hallintatasolla palvelunestoa voi seurata liian tiheistä reitityspäivityksistä, liiallisesta reititysinformaatiosta tai väärästä reititysinformaatiosta. Kun RFC 4111:n mukaisesti jätetään virtuaaliverkon sisäisistä syistä johtuvat seikat huomiotta, tarkastellaan vain, voiko yhteenliittämismalli aiheuttaa tai altistaa edellä mainittuja uhkia. Reitityspäivitykset generoituvat reititysmuutoksista (tässä yhteydessä siitä, minkä PE:n takaa tietty asiakasosoite löytyy), eikä yhteenliittämismallilla ole tähän

vaikutusta[62]. Toisaalta jokin väärä taho voisi syöttää tahallaan reittimuutoksia. Tämä taas liittyy siihen, mitä tahoja signalointiin ylipäänsä pääsee mukaan. Tämä on käsitelty luvussa 4.4.1 (kriteeri #8). Liialliseen ja väärään reititysinformaatioon pätee sama: yhteenliittämismallilla on vaikutusta korkeintaan siihen, voiko ylimääräinen taho päästä syöttämään informaatiota reititykseen. Kaikki palvelunestoon liittyvät kriteerit löytyvät jo muiden kriteerien alta.

4.5.2.2 Suojautumista lähdetietojen väärentämistä vastaan

Lähdetiedoilla tarkoitetaan tietylle virtuaaliverkon toimipisteelle tulevien datapakettien otsikkotietojen osoittamaa paketin alkuperää, yleensä sen IP-osoitetta ja Mac-osoitetta. Datapaketeille voidaan reitittimissä tehdä oikeellisuustarkastuksia (esimerkiksi uRPF-tarkastus); VPN-kontekstissa operaattori voi tehdä tämän vain leimaamattomalle paketille. Jos tällainen tarkistus halutaan tehdä AS-rajalla, saadaan kriteeri:

#21. Onko VPN-liikenne AS-rajalla leimaamatonta?

Lisäksi väärennetyillä lähettäjätiedoilla voi tulla liikennettä kokonaan virtuaaliverkkoon kuuluvilta lähettäjiltä. Tämä on käsitelty kohdassa.4.5.1.3.

4.5.3 Yksityisyys

4.5.3.1 Virtuaaliverkon sisäisen liikenteen tarkkailun estäminen ulkopuolelta

Sen lisäksi, että virtuaaliverkkoon ja sieltä pois ei tule voida liikennöidä kuin erillisillä järjestelyillä, myöskään virtuaaliverkon liikenteen ”salakuuntelun” ei tule olla mahdollista (luvatta). Myöskään verkon liikenteen tarkkailu ilman varsinaisen sisällön ”kuuntelua” ei ole toivottavaa. Tällaista tarkkailua voisi olla esimerkiksi verkon liikennemäärien tai yhteyksien osapuolten tietojen saanti. Salakuuntelu on periaatteessa mahdollista joko matkan varrella olevissa reitittimissä tai linkeillä. Myös kopioimalla ja ohjaamalla liikennettä johonkin ulkopuoliseen laitteeseen voidaan liikennettä kuunnella. Yhteenliittämisessä:

- Liikenne ei saa tarpeettomasti vuotaa AS:n ulkopuolelle.
- Ulkopuolinen ei saa päästä käsiksi operaattorin omaan verkkoon.
- Ulkopuolisen pääsy hallintatietoihin pitää olla tarkkaan rajattu.

[62] Yhteenliittämismallilla voi olla vaikutusta esimerkiksi virhetilanteessa, jos se vaikuttaa myös topogiaan – ei muuten.

Liikenteen, jonka pitäisi pysyä AS:n sisällä, vuotaminen sen ulkopuolelle vaatii joko sitä, että kahden samassa AS:ssä olevan PE:n välinen kuljetustunneli kulkee AS:n ulkopuolella tai että VPN:n sisällä liikenne ohjautuu väärin (egress-PE lähettää sen väärään kuljetustunneliin). Sisäisen liikenteen vuotaminen AS:n ulkopuolelle vaatii AS:n sisäisen reitityksen onnistunutta murtamista[63]. Useamman AS:n tapauksessa voi joku operaattori yrittää kaapata toisen operaattorin liikennettä, kuten luvun 5.4.1 kriteerissä #3 sanotaan. VPN:n sisällä liikenne ohjautuu eri VPN-tyypeissä eri lailla. L3-VPN:issä liikenteen ohjaus perustuu VPN-signaloinnissa välitettävään reititystietoon ja VPLS:ssä MAC-osoitteiden oppimiseen.

Kaksi muuta uhkaa liittyvät operaattorin hallinnan ja tietoturvakäytäntöjen järjestämiseen. Nämä on käsitelty alaluvussa 4.4.8.

Liikenteen ”varastaminen” BGP/MPLS IP-VPN:ssä

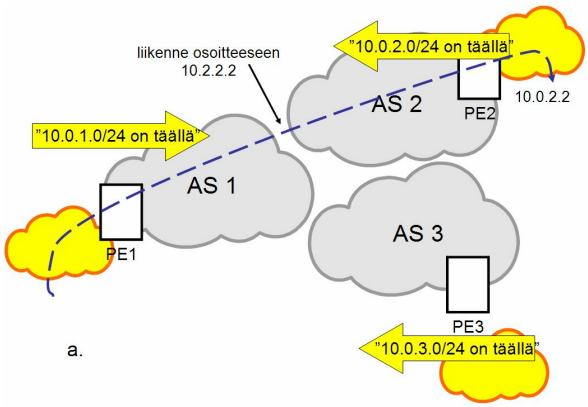
RFC 4364:n kuvaamassa L3-VPN:ssä liikenne välitetään toimipisteestä toiseen BGP-protokollan välittämän reititystiedon mukaisesti. Toimipisteiden välillä virtuaaliverkon sisällä kukin paketti lähetetään sitä toimipistettä kohti, jossa on BGP-reitityksen mukaan parhaiten kohdeosoitetta vastaava osoite (eli pisin yhteinen verkko-osa). Koska osoitteet mainostetaan usein ryhminä (aliverkkoina), on yleensä mahdollista mainostaa tarkempia osoitteita ja siten parempaa reittiä mille tahansa yksittäiselle aliverkolle tai päätteelle[64]. Kuvissa 34 ja 35 esimerkiksi PE3 mainostaa osoitetta 10.0.2.2 tarkemmalla osoitemainostuksella kuin PE2, jonka takana osoitteen haltija oikeasti on. Näin kaikki PE1:sen takana olevista toimipisteistä osoitteeseen 10.0.2.2 menevä liikenne meneekin PE3:lle. PE3 voi lähettää liikenteen edelleen PE2:lle (ja kerätä itse samalla haluamansa tiedot tai monistaa koko datavirran kolmanteen liitäntään). Tällaista liikenteen kierrätystä asiakkaan on mahdoton havaita, sillä runkoverkon osuus on virtuaaliverkolle näkymätön. PE-reitittimissä tämä voidaan havaita tarkkailemalla BGP-reititystä tai VRF-taulua. Vastaavasti se voidaan estää kahdella eri tavalla:

- määrittelemällä, että tiettyä bittimäärää pidemmillä verkkomaskeilla varustettuja reittejä ei hyväksytä, tai
- määrittelemällä tarkasti mitä reittejä mistäkin PE:stä hyväksytään.

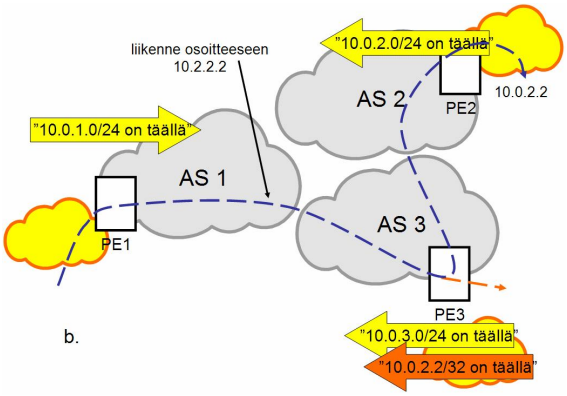
---

[63] Kuljetustunnelit muodostuvat PE-reititinten loopback-osoitteiden perusteella. Nämä osoitteet näkyvät AS:n sisäisessä reitityksessä (IGP) tarkimmalla mahdollisella verkkomaskilla (/32), joten niitä ei voi ohittaa ulkoisilla BGP-mainostuksilla.

[64] Vain osoitteille, jotka mainostetaan jo valmiiksi pisimmällä mahdollisella verkkomaskilla (IPv4:ssa 32-bittisellä ja IPv6:ssa 128-bittisellä), ei ole mahdollista mainostaa tarkempia reittejä.



Kuva 34. L3-VPN:n normaali toiminta



Kuva 35. Liikenteen varastaminen L3-VPN:ssä

Mainitut keinot vaativat asiakasreitityksen politiikkaan puuttumista[65] ja asiakasreitityksen ylläpitoa PE-reitittimissä. Mallissa A VPN-reititys ”putoaa pois” VPN-reitityksestä rajareititinten välillä, jossa voidaan käyttää muutakin reititystä kuin BGP:tä. Nämä toiset protokollat eivät tuo parempia suodatusominaisuuksia kuin BGP (eivätkä huonompia, koska BGP:tä käytetään joka tapauksessa AS:n sisällä). Kaikissa malleissa VPN-reittien suodatus on siis mahdollista ainakin naapuri-AS:n (peerauskumppanin) perusteella. Alkuperä-PE:n perusteella tehtävä suodatus on mahdollista vain silloin kun tieto alkuperästä säilyy (lähinnä mallit C ja D, jossa next-hop kertoo tämän). Suurin kysymys on kuitenkin:

#22. Signalointikumppanien varmistaminen

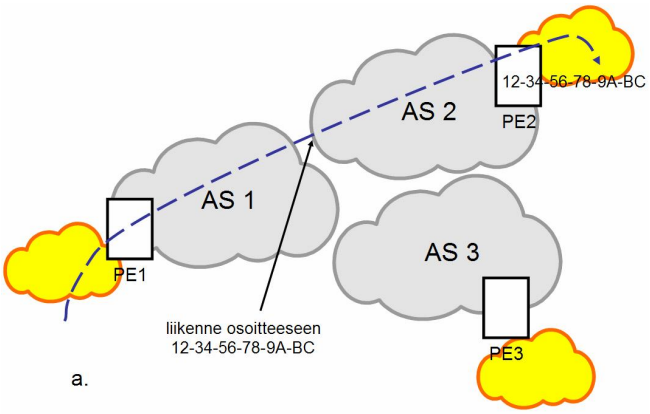
#23. Signalointitiedon alkuperän varmistaminen

---

[65] Ensin mainittu keino johtaa käytännössä kiinteämittaisten prefixien käyttöön (muuten jää osoitteita, joita voi houkutella väärille reiteille). Jälkimmäinen vaatii asiakasosoiteavaruuksien konfiguroimista route mapeihin, mikä johtaa ”puolikiinteään” reititykseen (reititys tapahtuu dynaamisella BGP:llä, mutta sisältö on konfiguraatioilla sidottu).

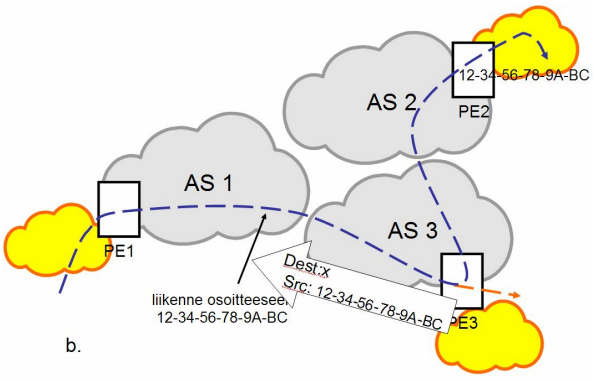
Liikenteen ”varastaminen” VPLS:ssä

Toisin kuin L3-VPN:ssä, VPLS:ssä ei vaihdeta reititystietoa. VPLS:ssä sen valinta, mihin toimipisteestä tuleva paketti kytketään, perustuu pakettien otsikkotiedon opiskeluun kussakin PE-laitteessa [Kom07][Las07]. Kuva 36 esittää tilannetta, jossa PE:t ovat oppineet, että MAC-osoite 12-34-56-78-9A-BC on PE2:n takana (VPLS:n toiminta käydään läpi kappaleessa 2.7). Kukin ko. VPLS:ää palveleva PE oppii tämän itsekseen, eikä tätä opittua tietoa vaihdeta muiden PE-reititinten kanssa[66]. Vaikka osoite on kertaalleen opittu, voi pahantahtoinen osapuoli VPLS:ssä lähettää liikennettä väärennetyllä lähde-MAC-osoitteella ja saada näin muut PE:t oppimaan, että kyseinen osoite onkin sen takana (kuvat 36 ja 37). Näin ”paha” PE (kuvassa PE3) saa tähän MAC-osoitteeseen tarkoitetun liikenteen itselleen. VPLS-määrittelyn mukaan tilanteissa, joissa sama MAC-osoite näkyy useamman yhteyden takaa, käytetään sitä, josta on viimeksi tullut liikennettä [Kom07][Las07]. Aivan kuten L3-VPN:ssä, ”paha” PE voi lähettää liikenteen edelleen oikealle vastaanottajalle, jolloin oikea vastaanottaja ei edes huomaa mitään. VPLS-palvelun luonteesta johtuen ”paha” PE saa näin myös kyseisen yhteyden paluuliikenteen itselleen, koska muut PE:t oppivat virheellisesti, että lähettäjä oli ”pahan” PE:n takana.



Kuva 36. VPLS:n normaali toiminta

[66] Poikkeuksena on mahdollinen MAC-osoitteiden poistaminen ”MAC Address Withdrawal”-viestillä. [Las07]



Kuva 37. Liikenteen varastaminen VPLS:ssä

”Pahan” PE:n on helppo saada VPLS-palvelussa käytössä olevat MAC-osoitteet selville, sillä ”uuteen[67]” osoitteeseen menevä liikenne lähetetään aina kaikille. ”Paha” PE voi myös aktiivisesti ajaa VPLS-palvelun tilaan, jossa kaikki liikenne lähetetään kaikille. Tämä tapahtuu lähettämällä liikennettä moniin eri MAC-osoitteisiin ja monista MAC-osoittteista, jolloin VPLS:lle varatut kytkentätaulut täyttyvät ja VPLS siirtyy yleislähetystilaan. Tämä ongelma voidaan kiertää olemalla käyttämättä MAC-osoitteiden oppimista ja käyttämällä kiinteitä MAC-tauluja sen sijaan. Tämä ratkaisu ei skaalaudu kovin monelle MAC-osoitteelle, eikä usein vaihtuville MAC-osoitteille. Kiinteiden MAC-taulujen käyttö ei ole sidoksissa yhteenliittämistapaan. Sen sijaan, siihen, ketkä pääsevät liikennöimään VPN:ään, yhteenliittämistavalla voi olla merkitystä. (Tätä kontrolloidaan VPN-signaloinnilla ja autodiscoveryllä). Kriteeriksi tältä osin tulee:

#24. Miten voidaan varmistaa, että vain luotetut tahot pääsevät VPN-signalointiin?

4.5.3.2 Virtualiverkon rakenteen (ja olemassaolon) pitäminen ulkopuolisilta salassa

Virtuaaliverkon rakenteella voidaan tarkoittaa kahta seikkaa: missä virtuaaliverkon toimipisteet ovat ja mitä (osoitteita) nämä toimipisteet sisältävät. Toimipisteiden lukumäärä ja sijainti (PE:n tarkkuudella) selviää autodiscovery-signaloinnista, paitsi niissä tapauksissa, joissa AS-kohtainen VPN-signaloinnin aggregointi piilottaa tämän tiedon. L3-VPN:ssä myös tieto siitä, mitä osoitteita käytetään missäkin toimipisteessä,

[67] ”Uudella” MAC-osoitteella tarkoitetaan tässä osoitetta, joka ei löydy kyseisen PE-reitittimen kytkentätaulusta. Tämä johtuu joko siitä, että osoitteeseen ei ole liikennöity aiemmin tai siitä, että kytkentätaulun tieto on kerinnyt vanhentua.

välitetään VPN-signaloinnin mukana. Sen sijaan VPN-signalointi ei kuljeta tietoa siitä, mikä asiakas käyttää kyseistä VPN:ää[68]. Kriteerit:

#25. Aggregoidaanko VPN-signalointi AS-kohtaisesti?

#26. Miten varmistetaan, etteivät ulkopuoliset ”kuule” VPN-signalointia?

4.5.4 CE-laitteen luotettava tunnistaminen

AS:ien yhteenliittäminen ei vaikuta CE-laitteiden luotettavaan tunnistamiseen, joten sitä ei käsitellä tässä työssä.

4.5.5 Eheys

RFC 4111 määrittelee eheyden: *”tieto pitää turvata siten, että sitä ei voi muuttaa matkalla tai, jos tietoa on muutettu, vastaanottaja voi havaita sen”*. Eheys on mahdollista varmistaa salaamalla tai allekirjoittamalla välitettävä tieto. Yleisesti suositaan salauksen käyttöä, sillä se takaa eheyden lisäksi myös yksityisyyden. VPN-liikenne voidaan salata monin tavoin, joista yleisin on käyttää IPsec-salattuja yhteyksiä. IPsec-yhteyksiä voi käyttää millä tahansa yhteysvälillä; sitä voi käyttää joko päästä-päähän (päätelaitteiden välillä) tai vain jollain välillä (esimerkiksi vain jaetussa pääsyverkossa CE-PE-välillä). Salatun yhteyden voi toteuttaa joko suoraan kahden pisteen välisenä (esimerkiksi CE-CE-väleillä) tai ketjutettuna (kukin CE-PE-väli erikseen ja PE-PE-välit erikseen). Koska VPN-palvelu on asiakkaan liikenteen kannalta läpinäkyvä, pääte- ja CE-laitteiden väliset suorat tunnelit toimivat myös virtuaaliverkoissa, jotka on muodostettu useamman AS:n yhteenliittymän yli. Sen sijaan eroja on, jos halutaan tehdä tunnelit PE-laitteiden välille. Kriteeri:

#27. Onko yhteenliittämismallissa mahdollista tehdä IPsec-tunneleita PE-laitteiden väleille?

[68] Asiakas voidaan päätellä välillisesti, jos signaloinnissa välitetään tietoa asiakkaalle rekisteröidyistä julkista IP-osoitteista. Myös VPN:n rakenteesta voidaan joissain tapauksissa päätellä asiakas.

4.5.6 VPN-liikenteen uusiokäyttö haitallisessa tarkoituksessa (Anti-replay)

VPN-liikenteen uusiokäyttö hyökkäysmielessä edellyttää pääsyä VPN:n liikennekerrokselle, jotta liikenne voitaisiin tallentaa. Liikenteen lähettäminen virtuaaliverkkoon vaatii lisäksi yksisuuntaisen yhteyden. Nämä tietoturvariskit on käsitelty kohdissa 4.5.1 ja 4.5.3.

4.6 Yhteenveto turvallisuuskriteereistä

Edellisissä alaluvuissa 4.4 ja 4.5 käsiteltiin leimakytkentäisten virtuaaliverkkojen tarjoamista tietoturvallisuuden näkökulmasta. Tavoitteena oli saada kerättyä konkreettisia kriteereitä, joilla eri yhteenliittämistapoja on mahdollista vertailla keskenään. Tarkastelu tuotti yhteensä 27 kriteeriä. Osa kriteereistä on samoja, vaikka niihin päädyttiin eri lähtökohdista.

Kriteerit #4 ja #14 ovat samat, kuten myös #9, #16 ja #19, #8 ja #17, #11 ja #27, #13 ja #20 sekä #22 ja #26. Lisäksi kriteerin #21 voi sisällyttää kriteeriin #13. Kriteeri #22 on sisällöllisesti käsitelty kriteerin #7 yhteydessä, kuten myös kriteeri #24 kriteerin #8 yhteydessä. Kriteeri #18 ei puolestaan ole tietoturvallisuuskriteeri eikä kriteeri #23 erottele eri yhteenliittämismalleja toisistaan.

Mielenkiintoinen yksityiskohta on, että kriteerit #18 ja #25 ovat käytännössä toistensa vastakohtia, jolloin yhdessä suhteessa tietoturvallinen malli voi olla toisessa suhteessa tietoturvattomampi.

Edellä läpikäydyn karsinnan jälkeen jäljelle jää 17 kriteeriä, jotka on listattu seuraavan alaluvun taulukossa

4.7 Vertailuun valitut kriteerit taulukkona

Oheisessa taulukossa 6 on koottuna seuraavan luvun vertailussa käytettävät kriteerit, jotka on koottu ja muokattu edellä mainituista kriteereistä. Vertailun jälkeisissä johtopäätöksissä pohditaan, mikä käytännön merkitys näillä on.

Taulukko 6. Vertailuun valitut kriteerit

Kriteerin numero vertailussa:	**Kriteerin tunniste aiemmin tässä luvussa:**	**Kriteeri:**	**Alaluvut, joissa kriteeri on perusteltu:**
1	#1	Voidaanko vastaanotettavien VPN-reittimainostusten määrää rajoittaa muuten kuin AS-kohtaisesti?	4.4.1
2	#1	Voidaanko vastaanotettavien IP-reittimainostusten määrää rajoittaa muuten kuin AS-kohtaisesti?	4.4.1
3	#2	Voidaanko vastaanotettavien VPN-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?	4.4.1
4	#2	Voidaanko vastaanotettavien IP-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?	4.4.1
5	#3	Onko VPN-palvelu suojassa vääriltä "globaaleilta" IP-osoitemainostuksilta?	4.4.1
6	#4, #14	Voidaanko PE- ja muiden reitittimien osoitteet jättää mainostamatta muihin AS:in?	4.4.1, 4.4.7
7	#5	Voidaanko PE- ja muissa runkoverkon reitittimissä käyttää yksityisiä IP-osoitteita?	4.4.1
8	#6	Tarvitseeko runkoreitittimissä olla tunnelien päätepisteitä, joihin voi liikennöidä AS:n ulkopuolelta?	4.4.1
9	#7, #22, #26	Kuinka monta signalointikumppania vaaditaan per kumppani-AS?	4.4.1, 4.5.3.1, 4.5.3.2

10	#8, #17, #24	Onko VPN-signalointikumppanina suoraan kohde-PE, vai käytetäänkö signaloinnissa välittäviä reitittimiä?	4.4.1, 4.5.1.3, 4.5.3.1
11	#9, #16, #19	Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?	4.4.1, 4.5.1.2, 4.5.1.3
12	#10	Voidaanko rajareititinten välinen yhteys suojata käyttäen IPsec:iä?	4.4.2
13	#11, #27	Voidaanko PE-PE–yhteydet suojata käyttäen IPsec:iä?	4.4.2, 4.5.5
14	#12	Voidaanko rajareitittimessä tehdä VPN-kohtaista liikenteenrajoitusta?	4.4.2
15	#13, #20, #21	Onko rajareititin itse kaikkien leimojen myöntäjä, jotka toisesta verkosta tulevien pakettien leimapinoissa saa olla?	4.4.2.1, 4.5.1.3, 4.5.2.2
16	#15	Vain PE-reitittimiin on tehtävä asiakaskohtaisia määrityksiä	4.4.8
17	#25	Voidaanko VPN-kohtaista tietoa "laimentaa" aggregoidamalla sitä AS-kohtaisesti?	4.5.3.2

luku 5:
Vertailu

Luvussa 3 esitellyillä yhteenliittämistavoilla on eri vahvuuksia, joten vertailun perusteella ei voi sanoa parasta vaihtoehtoa jokaiseen tilanteeseen. Luvussa 2 on esitelty eri VPN-palvelut. Niiden yhdistäminen toimimaan yli AS-rajojen poikkeaa toisistaan, vaikka olenkin jaotellut ne neljän eri mallin alle. Tästä johtuen vertailussa on kohtia, joita joudutaan tekemään myös palvelukohtaisesti.

Edellisen luvun taulukoon 6 kootut kriteerit on käsitelty alaluvussa 5.1 joko yksitellen tai joissain tapauksissa pari kerrallaan. Alaluvussa 5.2 on yhteenveto vertailusta sekä taulukkona että sanallisesti.

5.1 Vertailu kriteerikohtaisesti

1 ja 2: Voidaanko vastaanotettavien VPN- ja IP-reittimainostuksien lähetystiheyttä rajoittaa muuten kuin AS-kohtaisesti?

Tässä työssä käsiteltävistä virtuaaliverkkopalveluista vain BGP-protokollaa ja leimakytkentää hyödyntävä IP-virtuaaliverkkopalvelussa mainostetaan reittejä, L2-VPN:issä näin ei tehdä. Toisaalta vain yhteenliittämismalleissa C ja D tarvitaan autonomisten alueiden välistä reititystä. Kummassakin tapauksessa reittien vaihtoon AS:ien välillä käytetään BGP-protokollaa[69]. BGP:ssä on yhteysvälikohtaisesti konfiguroitavissa parametri `MinRouteAdvertisementIntervalTimer` [Rek06], jota useammin reititin ei saa lähettää reitityspäivityksiä. Näin ollen välitöntä naapuria kauempana olevat reititysmuutokset eivät näy AS:ien välisessä reititysrajapinnassa lisääntyneinä reittimainostuksina. Tämä edellyttää tietysti sitä, että välittömään naapuriin voi luottaa. Naapurin lähettämiä liiallisia reititysmuutoksia vastaan on kehitetty häilyvien reittien vaimennus[70] (oma suomennos, *engl. BGP Route*

[69] Yhteenliittämismallissa A voidaan käyttää myös muita IP-reititysprotokollia kuin BGP:tä.

[70] Häilyvien reittien vaimennuksen hyödyllisyys on kyseenalainen nykytoteutuksissa. Lisää tietoa ja suosituksia käytöstä löytyy esimerkiksi RIPE:n suosituksesta 378 [Smi06].

Flap Damping) [Vil98]. Rankaisu perustuu siihen, että ”huonosti käyttäytyvän” naapurin kanssa ei jutella tiettyyn aikaan ja tämä aika pitenee, jos huono käytös jatkuu.

Mallissa A ei välttämättä vaihdeta reittejä AS:ien välillä lainkaan. Jos vaihdetaan, reittien vaihto tapahtuu jokaisessa VPN:ssä toisistaan riippumatta (kullakin on oma reititysprosessinsa, sillä jokainen VPN on ASBR-reitittimessä omassa VRI:ssään). Koska kyseessä on normaali IP-reititys, kaikki normaalit reittimainostusten rajoituskeinot ovat käytössä per VPN. Näin ollen häilyvien reittien takia jäähylle laitettu reititysyhteys häiritsee vain sitä virtuaaliverkkoa, jonka reititys on epävakaa.

Mallissa B VPN-reitit vaihdetaan ASBR-reititinten välillä käyttäen VPNv4-unicast-osoiteperhettä BGP:ssä. Kaikkia samojen AS:ien välisiä virtuaaliverkkoja koskeva reititys vaihdetaan siis samalla reititysyhteydellä. Näin ollen kaikki rankaisutoimet kohdistuvat kaikkiin näiden AS:ien välisiin virtuaaliverkkoihin.

Mallissa C VPN-reitit vaihdetaan RR-reititinten välillä käyttäen VPNv4-unicast-osoiteperhettä BGP:ssä. Kaikkia samojen AS:ien välisiä virtuaaliverkkoja koskeva reititys vaihdetaan siis samalla reititysyhteydellä. Näin ollen kaikki rankaisutoimet kohdistuvat kaikkiin näiden AS:ien välisiin virtuaaliverkkoihin. Mallissa C IP-reitit vaihdetaan ASBR-reititinten välillä käyttäen IPv4-unicast-with-labels-osoiteperhettä BGP:ssä. Kaikkia samojen AS:ien välisiä kuljetustunneleita koskeva reititys vaihdetaan siis samalla reititysyhteydellä[71]. Näin ollen kaikki rankaisutoimet kohdistuvat kaikkiin näiden AS:ien välisiin virtuaaliverkkoihin.

Mallissa D VPN-reitit vaihdetaan RR-reititimen ja PE-reititinten välillä käyttäen VPNv4-osoiteperhettä BGP:ssä. Kaikkia AS:en ja tietyn PE:n välisiä virtuaaliverkkoja koskeva reititys vaihdetaan siis samalla reititysyhteydellä. Näin ollen kaikki rankaisutoimet kohdistuvat vain kaikkiin AS:n ja tietyn PE:n välisiin virtuaaliverkkoihin. Mallissa D IP-reitit vaihdetaan ASBR-reititinten välillä käyttäen IPv4-unicast-osoiteperhettä BGP:ssä. Kaikkia samojen AS:ien välisiä kuljetustunneleita[72] koskeva reititys vaihdetaan siis samalla reititysyhteydellä[73]. Näin ollen kaikki rankaisutoimet kohdistuvat kaikkiin näiden AS:ien välisiin virtuaaliverkkoihin.

---

[71] Tämä yhteys voidaan toki varmistaa, jolloin varareitti on käytettävissä.

[72] Se, että kuljetustunnelit eivät käytä leimakytkentää ei vaikuta tähän.

[73] Tämä yhteys voidaan toki varmistaa, jolloin varareitti on käytettävissä.

3 ja 4: Voidaanko vastaanotettavien VPN- ja IP-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?

BGP-reitityksessä on mahdollista rajoittaa vastaanotettavien reittien määrää per reititysnaapuri. IETF ei ole määritellyt, miten liiallisiin reitteihin tulee reagoida, joten reititinvalmistajien ratkaisut poikkeavat toisistaan. Cisco Systemisin reitittimiä käytettäessä rankaistaan naapuria samoin kuin *heiluvien reittien tapauksessa* (Route Flap Damping), jos reittien määrä naapurilta ylittää määritellyn: liikaa reittejä lähettänyt naapuri laitetaan jäähylle [Cis07]. Juniper Networksin reititimiä käytettäessä reititin joko laukaisee hälytyksen (yleensä verkonvalvontaan) tai hylkää ylimääräiset reitit, jos reittien määrä naapurilta ylittää määritellyn [Jun05].

Kaikissa malleissa on mahdollista rajoittaa reittimainostuksia, mutta vain mallissa A vaikutus on mahdollista rajata tiettyihin virtuaaliverkkoihin.

5: Onko VPN-palvelu suojassa vääriltä "globaaleilta" IP-osoitemainostuksilta?

Väärät globaalit IP-reititysmainostukset ovat mahdollisia vain malleissa C ja D, sillä vain niissä käytetään globaaleja mainostuksia.

6: Voidaanko PE- ja muiden reitittimien osoitteet jättää mainostamatta muihin AS:in?

Runkoverkon reititinten (muiden kuin ASBR:n) osoitteita on mainostettava muihin AS:iin vain malleissa C ja D. Näissä on mainostettava inter-AS-PE:iden osoitetta, johon kuljetustunneli päättyy ja lisäksi RR:n osoitetta, jonka kanssa naapuri muodostaa signalointiyhteyden.

7: Voidaanko PE- ja muissa runkoverkon reitittimissä käyttää yksityisiä IP-osoitteita?

Runkoverkon osoitteiden, jotka edellisen kriteerin kohdalla mainittiin, on syytä olla julkisesta osoiteavaruudesta operaattorille allokoituja. (Muut runkoverkon osoitteet voivat olla vaikka yksityisestä osoiteavaruudesta). Tällä vältetään päällekkäiset osoitteet ja pidetään osoitesuodatussäännöt mahdollisimman yksinkertaisina[74]. Jos yhteenliittyvät verkot kuuluvat samalle operaattorille, voidaan tästä säännöstä joustaa.

[74] Osoitteet, jotka kuuluvat yksityiseen osoiteavaruuteen, suodatetaan yleensä AS-rajalla.

8: Tarvitseeko runkoreitittimissä olla tunnelien päätepisteitä, joihin voi liikennöidä AS:n ulkopuolelta?

Mallissa A kaikki AS-rajan yli olevat yhteydet päättyvät jonkin sellaisen virtuaaliverkon VRI:hin, jolla on inter-AS-VPN. Kaikki niitä pitkin tuleva liikenne joutuu siis runkoverkon ulkopuolelle riippumatta pakettien otsakkeiden rakenteista tai sisällöstä.

Mallissa B kaikilla AS-rajan yli tulevilla paketeilla tulisi olla leima, jonka perusteella ne kuuluvat tiettyihin inter-AS-VPN:iin ja kaikki muu liikenne voidaan hylätä. Teoriassa liikenne ei siis voi päästä runkoverkonlaitteisiin. Käytännön toteutuksissa esimerkiksi Cisco Networksin reitittimissä tilanne ei kuitenkaan ole tämä. Reititinkohtaisten leimojen käytöstä johtuen ASBR hyväksyy mistä tahansa leimakytketystä liitännästä leimatun paketin, jonka päällimmäisen leiman se osaa tulkita, riippumatta siitä, onko tätä leimaa mainostettu kyseiseen liitäntään [Beh05].

Mallissa C kaikilla AS-rajan yli tulevilla paketeilla tulisi olla joko inter-AS-PE:hen, VPLS-hubiin tai inter-AS:ään käytettyyn reittiheijastimeen johtavaan leimapolkuun kuuluva leima. Tämän lisäksi – kuten edellä selitettiin – malli C voi olla myös avoin muille ASBR:n tietämille leimoille, vaikka niitä ei olisikaan mainostettu toiseen AS:ään.

Mallissa D ei välitetä leimoja AS:ien välillä, mutta siinä PE-laitteissa on avoimia[75] tunnelinpäitä.

9: Kuinka monta signalointikumppania vaaditaan per kumppani-AS?

Mallissa A signalointiyhteyksiä tarvitaan sama määrä kuin on inter-AS-VPN:iä. Riippuen ASBR:ien kapasiteetista nämä voidaan kaikki hoitaa yhdellä ASBR-kumppanilla per kumppani AS.

Mallissa B tarvitaan vain VPN-signalointi AS:ien välille. Tämä tarkoittaa BGP-yhteyttä L3-VPN:ille ja LDP-yhteyttä L2-VPN:ille. ASBR:ien kapasiteetista riippuen voidaan kaikki hoitaa yhdellä ASBR-kumppanilla per kumppani AS.

Mallissa C tarvitaan sekä IP- että VPN-signalointi AS:ien välille. IP-signalointi voidaan hoitaa yhdellä ASBR-kumppanilla per kumppani AS. L3-VPN:ien signalointi voidaan hoitaa yhdellä RR-RR-yhteydellä per AS-pari. VPLS:iä varten tarvitaan lisäksi yhdet yhteydet VPLS-hubien välille per AS-pari ja VPWS:iä varten tarvitaan

[75] Avoimuus riippuu käytetystä tunnelointiprotokollasta.

yhteydet kaikkien inter-AS-PE:iden välille, joiden välillä kyseistä palvelua käytetään. Varmistettuja yhteyksiä haluttaessa edellä mainitut yhteydet tulee varmistaa[76].

Mallissa D tarvitaan sekä VPN- että IP-signalointi AS:ien välille. IP-signalointi voidaan hoitaa yhdellä ASBR-kumppanilla per kumppani AS. L3-VPN-signalointia varten pitää muodostaa yhteys erikseen jokaiseen PE-reitittimeen oman AS:n ulkopuolella. VPLS-signalointia varten tarvitaan samoin yhteys erikseen jokaiseen PE-reitittimeen. VPWS:iä varten tarvitaan yhteydet kaikkien inter-AS-PE:iden välille, joiden välillä kyseistä palvelua käytetään.

10: Onko VPN-signalointikumppanina suoraan kohde-PE, vai käytetäänkö signaloinnissa välittäviä reitittimiä?

L3-VPN:ssä kaikissa muissa kuin mallissa D käytetään välittäviä reitittimiä (joko ASBR:ää tai RR:ää), jonka kanssa VPN-signalointitietoa vaihdetaan. L2-VPN:issä sekä mallissa C että D vaihdetaan VPN-signalointitietoa suoraan PE-reitittimen kanssa (poikkeuksena H-VPLS:ssä, jos naapuri-AS:ssä on hubi).

11: Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?

Tämä on L3-VPN-spesifinen kriteeri. Kaikissa muissa malleissa, paitsi mallissa A, kohdesuotimet säilyvät reittimainostuksissa, jolloin niitä on mahdollista käyttää suodatuksessa joko rajareitittimissä tai reittiheijasimissa.

12: Voidaanko rajareititinten välinen yhteys suojata käyttäen IPsec:iä?

IPsecin käyttö rajareitittimien välisellä linkillä on mahdollista kaikissa yhteenliittämismalleissa.

13: Voidaanko PE-PE–yhteydet suojata käyttäen IPsec:iä?

PE-PE-väleillä voidaan käyttää IPseciä, jos 1) PE:t voivat jutella IP-tasolla 2) PE:t tietävät, että kuljetustunnelin toinen pää on tietty PE. Nämä molemmat ehdot totetutuvat malleissa C ja D.

14: Voidaanko rajareitittimessä tehdä VPN-kohtaista liikenteenrajoitusta?

Mallissa A on asiakaskohtaiset (VPN-kohtaiset) liitännät, joten siinä asiakaskohtainen liikenteenrajoittaminen on mahdollista. Mallissa B on asiakaskohtaista signalointia ja asiakkaat voidaan tunnistaa leimoilla, periaatteessa olisi mahdollista tehdä asiakaskohtaista liikenteenrajoittamista. Tätä ei kuitenkaan ole reititinlaitavalmistajien

[76] L2-VPN:ien varmistaminen pitää tehdä päästä-päähän.

toimesta tuettu. Malleissa C ja D ei asiakaskohtainen liikenteentunnistaminen käytännössä onnistu, joten niissä ei myöskään asiakaskohtainen liikenteenrajoitus onnistu.

15: Onko rajareititin itse kaikkien leimojen myöntäjä, jotka toisesta verkosta tulevien pakettien leimapinoissa saa olla?

Malleissa A ja D ei käytetä leimoja AS:ien välillä lainkaan[77], joten se on kaikkien leimojen myöntäjä. Mallissa B leimapinossa voi olla vain ASBR:n mainostamia leimoja. Mallissa C paketeissa sen sijaan on useampi leima, joista ASBR tietää vain päällimmäisen merkityksen.

16: Vain PE-reitittimiin on tehtävä asiakaskohtaisia määrityksiä

Vain mallissa A on tarve tehdä asiakaskohtaisia määrityksiä muualle kuin PE-reitittimiin. Muissa malleissa VPN-signalointi huolehtii toimipisteiden välisestä signaloinnista ja liikennöinnistä automaattisesti.

17: Voidaanko VPN-kohtaista tietoa "laimentaa" aggregoimalla sitä AS-kohtaisesti?

Malleissa A ja B VPN-signalointi aggregoidaan rajareitittimessä. Mallissa C aggregointi tapahtuu RR:ssä (L3-VPN) tai VPLS-hubissa (VPLS), VPWS:n osalta signalointia ei aggregoida. Mallissa D aggregointia ei tehdä.

[77] Poikkeuksena mallissa A on CsC, jossa leimat ovat VPN:n sisäisiä ja mallissa D enkapsuloinnin sisällä olevat leimat, joita ei käytetä runkoverkon kytkennässä lainkaan.

5.2 Vertailun yhteenveto

Oheisessa taulukossa 7 on esitettynä edellisten alalukujen tiedot taulukkona. Väreistä kirkkaan vihreä tarkoittaa tietoturvallisuuden kannalta toivottavaa, tummanpunainen ei-toivottua toimintaa, keltainen tarkoittaa, että sinänsä ei-toivottu toimintatapa on kierrettävissä ja oranssi, että ei-toivottu toiminta luoteeltaan vähäistä.

Taulukko 7. Vertailun yhteenveto taulukkona

#	Kriteeri	Malli A	Malli B	Malli C	Malli D
1	Voidaanko vastaanotettavien VPN-reittimainostusten taajuutta rajoittaa muuten kuin AS-kohtaisesti?	kyllä (per VPN)	ei	ei	kyllä (per PE)
2	Voidaanko vastaanotettavien IP-reittimainostusten taajuutta rajoittaa muuten kuin AS-kohtaisesti?	ei tarvetta	ei tarvetta	ei	ei
3	Voidaanko vastaanotettavien VPN-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?	kyllä (per VPN)	ei	ei	kyllä (per PE)
4	Voidaanko vastaanotettavien IP-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?	ei tarvetta	ei tarvetta	ei[1]	ei[1]
5	Onko VPN-palvelun toiminta suojassa vääriltä "globaaleilta" osoitemainostuksilta?	kyllä	kyllä	ei	ei
6	Voidaanko PE- ja muiden reitittimien osoitteet jättää mainostamatta muihin AS:in?	kyllä	kyllä	ei	ei
7	Voidaanko PE- ja muissa runkoverkon reitittimissä käyttää yksityisiä IP-osoitteita?	kyllä	kyllä	ei	ei
8	Tarvitseeko runkoreitittimissä olla tunnelien päätepisteitä, joihin voi liikennöidä AS:n ulkopuolelta?	ei	kyllä[2]	kyllä	kyllä

9	Kuinka monta signalointikumppania vaaditaan per kumppani-AS?	1 per Inter-AS-VPN	2 per AS	3 per AS + 1 per VPWS-yhteys	1 per AS + 1-2 per kohde-PE + 1 per VPWS-yhteys
10	Onko VPN-signalointikumppanina suoraan kohde-PE?	ei	ei	ei / riippuu[3]	kyllä
11	Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?	ei	kyllä	kyllä	kyllä
12	Voidaanko rajareititinten välinen yhteys suojata käyttäen IPsec:iä?	kyllä	kyllä	kyllä	kyllä
13	Voidaanko PE-PE–yhteydet suojata käyttäen IPsec:iä?	ei	ei	kyllä	kyllä
14	Voidaanko rajareitittimessä tehdä VPN-kohtaista liikenteenrajoitusta?	kyllä	ei	ei	ei
15	Onko rajareititin itse kaikkien leimojen myöntäjä, jotka toisesta verkosta tulevien pakettien leimapinoissa saa olla?	kyllä	kyllä	ei	kyllä
16	Vain PE-reitittimiin on tehtävä asiakaskohtaisia määrityksiä	ei	kyllä	kyllä	kyllä
17	Voidaanko VPN-kohtaista tietoa "laimentaa" aggregoimalla sitä AS-kohtaisesti?	kyllä	osittain[4]	ei	ei

[1] Puhtaasti määrään perustuva suodatus katkaisee koko peerauksen, joten sen käyttö haittaa inter-AS-VPN:iä. Laadullinen suodatus on mahdollista normaalien BGP-käytäntöjen mukaisesti

[2] Tämänhetkisillä toteutuksilla suodatus ei onnistu käytännössä, vaikka reitittimellä on tarvittavat tiedot sen toteuttamiseksi.

[3] VPWS:llä ei käytetä välittäviä reitittimiä, L3-VPN:ssä ja VPLS:ssä voidaan käyttää

[4] Tarkka tieto suodattuu, mutta eri toimipisteille on eri leimat, joista voi päätellä toimipisteiden lukumäärän

5.2.1 Sanallinen yhteenveto

Taulukosta 7 voi laskea, että malli A:ssa on eniten vihreätä (12) ja vähiten (2) punaista ja vastaavasti mallissa C eniten punaista (11+2) ja vähiten vihreää (3). Malli B on vertailussa monin osin A:n kaltainen, mutta erojakin on: B saa 6 punaista, 9 vihreää ja yhden keltaisen merkinnän. Mallilla D vastaavasti on C:n ”pari”; sillä on C:tä hieman vähemmän punaisia kohtia (8+1) ja enemmän vihreitä (7) – vain yhdessä kriteerissä (#9) D on C:tä huonompi. Jos vertailun kriteereitä pidetään yhtä tärkeinä ja toisistaan riippumattomina, voidaan taulukosta laskea ”tietoturvallisuusjärjestys”: A, B, D, C. Kannattaa kuitenkin huomata, että kohdissa, joissa ”paras” (eli Mallin A mukainen) yhteenliittämistapa on saanut punaisen arvion, jollain muulla tavalla arvo on vihreä. Näin ollen parasta tapaa arvioidessa on syytä käydä tarpeita vastaavat kriteerit läpi. Liitteessä A palataan tähän.

luku 6:
Johtopäätökset

Johtopäätös-luku jakaantuu kolmeen osaan: Ensimmäisessä alaluvussa (6.1) käyn läpi vertailun tuloksia. Toisessa (6.2) käyn läpi tutkimuksen rajauksia ja pohdin niiden merkitystä. Kolmannessa (6.3) arvioin työn onnistumista kokonaisuutena.

6.1 Mitä vertailu kertoo?

Edellisen luvun vertailu kertoo, että yhteenliittämistavoilla on eroa – näiltä osin vertailun minimitavoite on täytetty. Tarkempi analyysi eroista on liitteessä A. Oheen olen koonnut tulokset yhteenliitämistavoista mallikohtaisesti omiksi alaluvuikseen.

6.1.1 Mallin A tietoturva

Malli A on tämän tutkielman mukaan kaikkein tietoturvallisin. Se läpäisee kaikki kriteerit, jotka koskevat operaattoria ja intra-AS-asiakkaita. Sillä ei ole näiden tietoturvaan liittyviä puutteita.

Inter-AS-asiakkaiden osalta havaitsin mallilla A kaksi puutetta. Nämä puutteet liittyvät kumppaniverkon sisäisen tietoturvan tasoon eli kumppanioperaattorin käytäntöjen tietoturvallisuuden tasoon. Tämän ohella mallin A ongelmana voi nähdä tietyn läpinäkyvyyden puutteen, koska sitä käytettäessä operaattorilla ei ole mitään näkyvyyttä toiseen verkkoon. Tämä koskee sekä reititystiedon alkuperää että mahdollisuutta PE-reititinten väliseen salaukseen.

Lisäksi mallissa A on pakko antaa myös transit-operaattorin osallistua VPN-signalointiin, mitä voidaan pitää joskus ei-toivottavana. Kaikki mainitut asiat voi kiteyttää, mallissa A kyseessä on *luottamuksen määrä operaattoreiden välillä koskien yhteisten asiakkaiden yhteyksiä*. Jos asiakas tietää, minkä verkkojen kautta hänen yhteytensä kulkevat, ja asiakas luottaan kaikkien näiden verkkojen (operaattoreiden) tietoturvaan, mallin A tietoturva on riittävä. Jos asiakas ei luota kaikkien operaattoreiden tietoturvaan, on mahdollista käyttää salausta CE-reititinten välillä.

6.1.2 Mallin B tietoturva

Mallilla B on operaattoria ja intra-AS-asiakkaita koskien kaksi puutetta. Näistä vakavampi liittyy mallissa B rajareitittimen puuttuvaan kykyyn suodattaa liikennettä sisään tulevien pakettien leimojen perusteella. Näin ollen *kaikki leimapolut, joihin rajareitin voi lähettää leimakytkettyä liikennettä, ovat avoinna myös naapuri-AS:ään*. Tämä haavoittuvuus liittyy leimakytkennän käytännön toteutukseen (ainakin Ciscon reitittimissä [Beh05]), eikä välttämättä koske kaikkia reititinvalmistajia[78]. Tämä turvallisuusaukko on myös mahdollista tukkia käyttämällä kahta ASBR-reititintä peräkkäin [Beh05].

Inter-AS-asiakkaiden tietoturvaan liittyen mallissa B on mallin A puutteiden lisäksi kaksi puutetta enemmän (kriteerit 1, 14; taulukko 7). Näistä ongelmallisin johtuu LDP-protokollan käytöstä verkkojen välillä. Tällä hetkellä siihen ei ole kehitetty vastaavia suojausmekanismeja kuin BGP:hen, joten naapurioperaattorin virhekonfiguraatio saattaa vaikuttaa LDP:n välityksellä rajan yli. Näin ollen *mallia B ei voi suositella, jos kumppanioperaattorin (ASBR:n) konfiguraatioden virheettömyyteen ei luoteta ja lisäksi AS:ien välillä käytetään LDP-protokollaa*. Käytännössä tämä tarkoittaa L2-VPN:iä, joita ei konfiguroida staattisesti. LDP-protokollaa kehitetään IETF:ssä edelleen erityisesti moniosaisiin virtuaalijohtimiin liittyen. Tämän standardointityön puitteissa siihen tullee inter-AS-käytöön liittyviä parannuksia.

Inter-AS-asiakkaiden osalta mallissa B on sama ongelma kuin mallissa A: pakko antaa myös transit-operaattorin osallistua VPN-signalointiin.

Malli B on kokonaisuutena varsin tietoturvallinen, mutta edellyttää isompaa luottamusta kumppaniin kuin malli A. Tietoturvan vaarantuminen edellyttää mallissa B, että välittömän kumppanin rajareitittimen tietoturva on vaarantunut – ongelmien hyödyntäminen kauempaa verkosta ei onnistu.

6.1.3 Mallin C tietoturva

Vertailussa mallista C löytyi eniten tietoturvaongelmia. Sillä on suurin osa mallien A ja B ongelmista, joskin läpinäkyvyys on parempi. Mallin C ongelmat liittyvät verkkojen yhteiseen hallintatasoon, sillä mallissa C joudutaan jakamaan sekä VPN-signalointi, IP-reititys että leimakytkentä verkkojen kesken. Reitityksestä tulevia ongelmia on

---

[78] Muiden valmistajien osalta en löytänyt asiasta mainintaa – niin kuin ei Ciscollakaan normaalimateriaalissa.

mahdollista lieventää käyttämällä IP-liikenteestä erillisiä rajareitittimiä VPN-liikenteelle.

Mallissa C ei voida tehdä kumppanilta piilotettua runkoverkkoa: ainakin PE-reititinten, VPLS-hubien ja reittiheijastimien osoitteiden tulee näkyä kumppanille ja näihin tulee myös olla pääsy kumppanin verkosta.

Isoin tietoturvaan liittyvä ongelma mallissa C ovat toiseen verkkoon johtavat kuljetustunnelin päät. Nämä ovat olemassa VPN-liikenteen kuljettamista varten, mutta rajareititin ei osaa päätellä yksittäisestä paketista, onko se VPN-liikennettä vai jotain muuta. Näin ollen toisesta AS:stä tulevan, kuljetusleiman alla olevan paketin sisältö, otsakkeet mukaan lukien, voi olla mitä vain. Tämä saattaa mahdollistaa pääsyn intra-AS-VPN:iin tai runkoverkon normaalisti suojattuihin kohteisiin. Tämän tyyppiset tietoturvaongelmat ovat erittäin haastavia, sillä ne vaativat kokonaisvaltaisempaa tietoturvan hallintaa kuin mitä verkkorajapinnassa on mahdollista tehdä. Kuvatun kaltainen liikenne voi alkaa mistä tahansa kumppanioperaattorin leimakytketyltä alueelta, mutta ei sen leimakytkemättömistä liitännöistä. Tässäkin on kyse siis luottamuksen tasosta kumppanioperaattoriin ja sen tietoturvakäytäntöihin.

Inter-AS-asiakkaiden tietoturvaan liittyen mallissa C on sama ongelma kuin mallissa B: *mallia C ei voi suositella, jos kumppanioperaattorin (ASBR:n) konfiguraatioden virheettömyyteen ei luoteta ja lisäksi AS:ien välillä käytetään LDP-protokollaa.* Mallissa C *väärä operaattori voi myös yrittää viedä VPN-liikennettä* mainostamalla toiselle operaattorille kuuluvan PE-reitittimen osoitetta. Tämä on mahdollista vain tietyissä verkkotopologioissa ja on estettävissä riippuen AS-topologiasta. CE-reititinten välistä salausta voidaan käyttää VPN-liikenteen yksityisyyden suojaamiseen myös tätä uhkaa vastaan. Transit-operaattoreiden suhteen malli C on malleja A ja B tietoturvallisempi: transit-operaattorin ei tarvitse osallistua VPN-signalointiin.

Mallissa C operaattori joutuu sekä jakamaan enemmän tietoa verkostaan kumppanille että luottamaan tämän tietoturvakäytäntöihin malleja A ja B enemmän. Se soveltuukin operaattorien väliseksi liitännäksi vain silloin kun operaattorit luottavat toisiinsa ”kuin itseensä”. Tietoturvan vaarantuminen edellyttää mallissa C, että jonkin kumppanin runkoverkon tietoturva on vaarantunut - ongelmien hyödyntäminen leimakytkettyjen runkoverkkojen ulkopuolelta ei onnistu. Kokonaisuutena tarkasteltuna malli C onkin nykyisin soveltuva operaattorin omien AS:ien väliseen liitäntään.

6.1.4 Mallin D tietoturva

Mallissa D VPN-liikenne kulkee suurelta osin Internet-liikenteen seassa. Siinä VPN-liikenne kärsii IP-reitityksen ja -liikenteen mahdollisista ongelmista – sekä tahallisista

tai tahattomista. Mallissa D on toisaalta mahdollista hyödyntää salausta sekä signaloinnin alkuperän että liikenteen varmistamiseen, jolloin transit-operaattorit eivät tiedä virtuaaliverkkojen toteutuksesta lainkaan.

Ottaen huomioon palvelun laadun takaamisen vaikeudesta johtuvat mahdolliset tietoturvaongelmat ja salauksen huonohkon skaalautuvuuden, on malli D tietoturvallinen malli, joka soveltuu rajoitettuihin toteutuksiin.

6.2 Tutkimuksen rajauksen onnistumisesta

Kun aloin suunnitella tätä tutkimusta, oli mielessäni ohjekirja operaattoreille virtuaaliverkkojen yhteenliittämisestä. Idea sellaisenaan oli liian laaja diplomityöksi, joten sitä oli kehitettävä ja rajattava. Rajauksia olivat: pitäytyminen leimakytkennässä; vain joidenkin virtuaaliverkkopalveluiden tarkasteleminen; yhteenliittämistapojen rajaaminen määrittelemällä; sekä operaattorinäkökulman käyttäminen ja tietoturvaan keskittyminen.

Tärkeimmät rajaukset olivat valitut virtuaaliverkkopalvelut ja tietoturva-aihepiiri; muut rajaukset olivat lähinnä seurasta näistä. Laajemmat perustelut rajauksille on annettu aiemmin tässä työssä. Lyhyesti sanottuna halusin mukaan kaikki oleelliset palvelut, jotta työstä tulisi ”yleispätevä”. Mielestäni ratkaisu oli onnistunut, vaikkakin se kasvatti työn pituutta ja teki siitä hieman vaikeamman hahmottaa. Tietoturvaan keskittyminen oli enemmän työn laajuudesta tullut vaatimus: ottamalla enemmän aihepiirejä mukaan olisi joko työn mitta kasvanut tai sen sisältö tullut yleisluontoisemmaksi. Kumpikaan ei olisi mielestäni ollut tavoiteltavaa. Tältä pohjalta pidän rajausta onnistuneena.

Tietoturvan sijasta yhteenliittämistä olisi ollut mielekästä tarkastella muistakin näkökulmista, kuten palvelun laadun, verkon hallinnan tai skaalautuvuuden näkökulmista. Nämä ovatkin hyviä jatkotutkimuksen aiheita, joihin tästä työstä löytyy jo paljon pohjamateriaalia.

Yhteenliittämistapojen osalta työssä käsitellyt neljä tapaa kattavat pääpiirteissään kaikki yleiset yhteenliittämistavat. Toki näiden tapojen sisälläkin joitakin asioita voidaan tehdä toisin esimerkiksi käyttämällä staattista reititystä ja leimojen allokointia dynaamisen sijaan. Nämä variaatiot eivät kuitenkaan vaikuta oleellisesti yhteenliittämistapojen tietoturvaan. Toisaalta IETF on vasta aloittanut yhteenliittämisen standardoinnin, mikä saattaa tuoda muassaan uusia yhteenliittämisen tapoja.

Kokonaisuutena pidän tutkimuksen rajauksia hyvin tarkoitustaan palvelevina – siis onnistuneina.

6.3 Jatkokehitettävää ja –tutkittavaa

Tämän tutkimuksen valossa erityisesti reititinten toteutuksissa on puutteita, jotka voivat olla esteinä paremmin skaalautuvien yhteenliittämistapojen (mallit B ja C) käytölle operaattorien välisissä leimakytkentää tukevissa liitännöissä. Erityisesti tämä koskee rajareitittimessä (ASBR) suoritettavaa liikenteen suodatusta. Nykytoteutuksissa on kaksi puutetta, joiden korjaaminen lisäisi niiden välisten leimakytkettyjen liitäntöjen tietoturvaa. Ensimmäinen on niiden pakettien suodattaminen, joiden leimaa ei ole mainostettu kyseiseen liitäntään. Toinen liittyy pakettien suodattamiseen uloimman leiman sisällä olevan paketin perusteella. Näistä ensimmäinen olisi toteutettavissa pienehköllä vaivalla, sillä samantyylistä suodatusta voidaan käyttää jo nykyisin IP-liikenteelle. Jälkimmäisen toteuttaminen on haastavampaa, mutta ei ylivoimaista.

Standardien osalta työ on yhteenliittämiseen liittyen kesken. Suurimmat puutteet ovat L2-VPN:issä ja erityisesti moniosaisissa virtuaalijohtimissa ja näiden automaattisessa signaloinnissa.

Jatkotutkimuskohteita leimakytkentäisten virtuaaliverkkojen yhteenliittämiseen liittyen voisivat olla esimerkiksi palvelun laadun varmistaminen useamman verkon ja operaattorin kesken tai palvelun hallinta useamman operaattorin yhteenliittymässä (esimerkiksi LSP-ping ja –traceroute toiminteet eivät toimi sujuvasti kaikilla yhteenliittämistavoilla). Myös skaalautuvuuteen ja virtuaaliverkkojen luomiseen useammassa autonomisessa alueessa liittyy monia kysymyksiä, joita voisi olla järkevää pohtia esimerkiksi diplomityön puitteissa.

6.4 Mietteitä diplomityön teosta

Tämän diplomityön tekoprosessi on ollut todella pitkä; laskentatavasta riippuen useampia vuosia. Tänä aikana sekä tutkimuksen aihe että organisaatio, jossa olen töissä, on muuttunut – itse asiassa useammankin kerran. Diplomityön teko työn ohella on osoittautunut erittäin haasteelliseksi. Varsinaisesti *tätä* tutkimusta olen tehnyt vajaan vuoden ajan. Vaikka tutkimuksen aihe liittyykin työhöni, se ei ole ollut osa varsinaista työtäni, joten olen tehnyt sitä lähinnä vapaa-ajalla. Haasteena on ollut löytää riittävän pitkiä yhtenäisiä aikoja uppoutua työn tekoon. Käytännössä työn valmistuminen on vaatinut pitkäjännitteistä ajankäyttöä ja huolellista vaiheittaista suunnitelmallisuutta. Luonnollisesti tämä on vaatinut asian sopimista sekä kotona että töissä.

Ajan kuluminen on asettanut myös toisenlaisia haasteita: on ollut otettava huomioon mahdollisuus, että aihe ei enää olekaan ajankohtainen – tai että siitä on jo julkaistu riittävästi, jolloin diplomityöhön ei jäisi enää omaa sanottavaa. Vaikka leimakytkennästä onkin kirjoitettu viime vuosina paljon, on eri verkkojen yhteenliittäminen aiheena jäänyt vähemmälle. Vuoden päästä tilanne on luultavasti toisin.

Ajan kulumista on ollut myös hyötyä. Olen saanut melkoisesti kokemusta leimakytkennän käytännön hyödyntämisestä ja mahdollisuuksista operaattoritoiminnassa. Se helpottaa sekä tämän työn tapaisen teoreettisen pohdiskelun tekemistä että sen merkityksen asettamista oikeaan asiayhteyteen.

Itse tutkimusaiheen lisäksi tämän työn tekeminen on opettanut minulle aiheen rajauksen ja tutkimusongelman konkretisoimisen merkitystä. Alussa luotin liikaa ajatukseen, että työ rajaa itsensä. Tosiasiassa kävi päinvastoin: mitä enemmän aiheeseen perehtyi, sitä enemmän siitä löytyi polkuja, joita seurata. Tällöin oli hyvä ottaa aikalisä ja kirkastaa tutkimuksen tavoite. Työn tekeminen olisi ollut helpompaa, jos tavoite olisi ollut yhtä kirkas alusta asti – toisaalta moni mielenkiintoinen asia olisi jäänyt selvittämättä.

Kokonaisuutena tutkimukseni täytti sille asettamani tavoitteet. Samaa voi sanoa koko diplomityön tekoprosessista. Se tuntuu näin taaksepäin katsoen työläältä, mutta mielekkäältä tavalta mitata osaamistaan.

LÄHDELUETTELO

[And01] Loa Andersson, Paul Doolan, Nancy Feldman, Andre Fredette & Bob Thomas, ”*LDP Specification*”, IETF RFC 3036, tammikuu 2001, 132 s.

[And02] Loa Andersson, Ross Callon, Ram Dantu, Paul Doolan, Nancy Feldman, Andre Fredette, Eric Gray, Juha Heinanen, Bilel Jamoussi, Timothy E. Kilty, Andrew G. Malis, Muckai K Girish, Tom Worster & Liwen Wu, "*Constraint-Based LSP Setup using LDP*", IETF RFC 3212, tammikuu 2002, 42 s.

[And05] Loa Andersson & Tove Madsen, "*Provider Provisioned Virtual Private Network (VPN) Terminology*", IETF RFC 4026, maaliskuu 2005, 20 s.

[Aug06] Loa Andersson, Eric C. Rosen, Waldemar Augustyn, Marty Borden, Juha Heinanen, Kireeti Kompella, Vach Kompella, Marc Lasserre, Pascal Menezies, Hamid Ould-Brahim, Vasile Radoaca & Tissa Senevirathne, "*Framework for Layer 2 Virtual Private Networks (L2VPNs)*", IETF RFC 4664, syyskuu 2006, 44 s.

[Aug06] Waldemar Augustyn & Yetik Serbest, “*Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks*”, IETF RFC 4665, syyskuu 2006, 32 s.

[Awd01] Daniel O. Awduche, Lou Berger, Der-Hwa Gan, Tony Li, Vijay Srinivasan & George Swallow, "*RSVP-TE: Extensions to RSVP for LSP Tunnels*", IETF RFC 3209, joulukuu 2001, 61s.

[Bat07] Tony Bates, Ravi Chandra, Dave Katz & Yakov Rekhter, "*Multiprotocol Extensions for BGP-4*", IETF RFC 4760, tammikuu 2007, 12 s.

[Bbn04] BBN Technologies, "Secure BGP Project (S-BGP)", tammikuu 2004, kotisivu: <http://www.ir.bbn.com/projects/s-bgp/>, viitattu 22.5.2007.

[Beh05] Michael H. Behringer & Monique J. Morrow, ”*MPLS VPN Security*”, Cisco Press, ISBN: 1-58705-183-4, kesäkuu 2005, 312 s.

[Beh06] Michael H. Behringer, "*Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)*", IETF RFC 4381, helmikuu 2006, 22 s.

[Beh07] Michael H. Behringer, ”*MPLS Security in Service Provider Networks*”, esitelmä, Networkers EMEA, helmikuu 2007, 76 s.

[Bit06] Nabil Bitar, Matthew Bocci & Luca Martini, ”*Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3)*”, IETF Internet Draft, keskeneräinen, viitattu versio: draft-ietf-pwe3-ms-pw-requirements-05.txt, kesäkuu 2006, 22 s.

[Boc06] Matthew Bocci & Stewart Bryant, ”*An Architecture for Multi-Segment Pseudo Wire Emulation Edge-to-Edge*”, IETF Internet draft, keskeneräinen, viitattu versio: draft-ietf-pwe3-ms-pw-arch-02.txt, lokakuu 2006, 20 s.

[Bra96] Scott O. Bradner, *"Internet Standards Process"*, IETF RFC 2026, lokakuu 1996. 36 s.

[Cal05] Ross Callon, ”*A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)*”, IETF RFC 4110, heinäkuu 2005, 82 s.

[Car05] Marco Carugi & Dave McDysan (toim.), Luyuan Fang, Ananth Nagarajan, Junichi Sumimoto & Rick Wilder, ”*Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs)*”, IETF RFC 4031, huhtikuu 2005, 50 s.

[Cis07] Cisco Systems, “*BGP Restart Session After Max-Prefix Limit*”, maaliskuu 2007, 22 s., saatavissa:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sbc27/ftbrsamp.pdf>, viitattu 1.4.2007.

[Dav00] Bruce Davie & Yakov Rekhter, “*MPLS: technology and applications*”, Morgan Kaufmann Publishers, ISBN 1-55860-656-4, toukokuu 2000, 287 s.

[Fan05] Luyuan Fang, "*Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)*", IETF RFC 4111, heinäkuu 2005, 45 s.

[Gil04] Vijay Gill, John Heasley & David Meyer, "*The Generalized TTL Security Mechanism (GTSM)*", IETF RFC 3682, helmikuu 2004, 11s.

[Gui01] Jim Guichard & Ivan Pepelnjak, "*MPLS and VPN Architectures*", Cisco Press. 1st edition (3rd printing). ISBN: 1587050021, maaliskuu 2001, 420 s.

[Hef98] Andy Heffernan, "*Protection of BGP Sessions via the TCP MD5 Signature Option*", IETF RFC 2385, elokuu 1998, 6 s.

[Iet06] IETF, ”*Layer 3 Virtual Private Networks (l3vpn) Charter*”, maaliskuu 2006, luettavissa: <http://www.ietf.org/html.charters/l3vpn-charter.html>, viitattu 22.5.2007.

[Iet07a] IETF, ”*Layer 2 Virtual Private Networks (l2vpn) Charter*”, maaliskuu 2007, luettavissa: <http://www.ietf.org/html.charters/l2vpn-charter.html>, viitattu 22.5.2007.

[Iet07b] IETF, ”*Pseudowire Emulation Edge to Edge (pwe3) Charter*”, maaliskuu 2007, luettavissa: <http://www.ietf.org/html.charters/pwe3-charter.html>, viitattu 22.5.2007.

[Iet07d] IETF, ”*Official Internet Protocol Standards*”, toukokuu 2007, luettavissa: <http://www.rfc-editor.org/rfcxx00.html>, viitattu 22.5.2007.

[Jun05] Juniper Networks, “*Routing Protocols Configuration Guide Release 7.3*”, kesäkuu 2005, 664 s., saatavissa: <http://www.juniper.net/techpubs/software/junos/junos73/swconfig73-routing/download/swconfig73-routing.pdf>, viitattu 22.5.2007.

[Kan99] Raimo Kantola. "*Integration of Routing and Switching; Label Switching & IP switching*", Tiedonvälitystekniikka II (S-38.122) luentomateriaalia, syksy 1999, 45 s., saatavissa: <http://www.netlab.tkk.fi/opetus/s38122/s99/kuudes.pdf>, viitattu: 21.4.2007.

[Kom07] Kireeti Kompella & Yakov Rekhter, “*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*”, IETF RFC 4761, tammikuu 2007, 28 s.

[Las07] Marc Lasserre & Vach Kompella, “*Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*” , IETF RFC 4762, tammikuu 2007, 31 s.

[Luo05] Wei Luo, Carlos Pignataro, Anthony YH Chan & Dmitry Bokotey, "*Layer 2 VPN Architectures*", 1st. Edition, Cisco Press, ISBN-10: 1-58705-168-0, ISBN-13: 978-1-58705-168-5, maaliskuu 2005, 648 s.

[Mal07] Andrew G. Malis, Luca Martini, Jeremy Brayley & Tom Walsh, "*Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service*", IETF RFC4816, helmikuu 2007, 5 s.

[Mal07b] Andrew G. Malis, Prayson Pate, Ron Cohen (toim.) & David Zelig, "*Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Circuit Emulation over Packet (CEP)*", IETF RFC 4842, huhtikuu 2007, 43 s.

[Mar06a] Luca Martini, Nasser El-Aawar, Giles Heron, Eric C. Rosen & Toby Smith, "*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*", IETF RFC 4447, huhtikuu 2006, 33 s.

[Mar06b] Pedro Marques, Ronald Bonica, Luyuan Fang, Luca Martini, Robert Raszuk, Keyur Patel & Jim Guichard, "*Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*", IETF RFC 4364, marraskuu 2006, 14 s.

[Mar06c] Luca Martini (toim.), Nasser El-Aawar, Giles Heron & Eric C. Rosen, "*Encapsulation Methods for Transport of Ethernet over MPLS Networks*", IETFRFC 4448, huhtikuu 2006, 24 s.

[Mar06d] Luca Martini, Claude Kawa & Andrew G. Malis, "*Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*", IETF RFC 4619, syyskuu 2006, 19 s.

[Mar06e] Luca Martini, Giles Heron, Eric C. Rosen & Andrew G. Malis, "*Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks*", IETF RFC 4618, syyskuu 2006, 26 s.

[Mar06f] Luca Martini, Jayakumar Jayakumar, Matthew Bocci, Nasser El-Aawar, Jeremy Brayley & Ghassem Koleyni, "*Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks*", IETF RFC 4717, joulukuu 2006, 40 s.

[Mar07] Luca Martini, Thomas D. Nadeau, Chris Metz, Mike Duckett, Vasile Radoaca, Matthew Bocci, Florin Balus & Mustapha Aissaoui, "*Segmented Pseudo Wire*", IETF Internet Draft, keskeneräinen, viitattu versio: draft-ietf-pwe3-segmented-pw-04.txt, helmikuu 2007, 38 s.

[Mor07] Thomas Morin (toim.), "*Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)*", IETF RFC 4665, huhtikuu 2007, 37 s.

[Nag04] Ananth Nagarajan, ”*Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)*”, IETF RFC 3809, kesäkuu 2004, 25 s.

[Pep03] Ivan Pepelnjak, Jim Guichard & Jeff Apcar, "*MPLS and VPN Architectures, Vol. 2*", Cisco Press, 1st edition, ISBN-10: 1587051125, ISBN-13: 978-1587051128, kesäkuu 2003, 504 s.

[Rag02] Gary L. Ragsdale & Ryan D. Lamm, "*Advancements in Photonic Network Architecture Migration: The Evolution and Deployment of Multiprotocol Label Switching (MPLS), Generalized Multiprotocol Label Switching (GMPLS), and Advanced Optical Switching*", National Communications System Technical Information Bulletin 02-4, toukukuu 2002, 59 s., saatavilla: <http://www.ncs.gov/library/tech_bulletins/2002/tib_02-4.pdf>, viitattu: 21.4.2007.

[Rah06] Juha Rahikainen, ”*MPLS-liikenteen Tietoturva*”, opinnäytetyö, Jyväskylän ammattikorkeakoulu, toukokuu 2006, 65 s.

[Ram07] Anantha Ramaiah, Randall R. Stewart & Mitesh Dalal, "*Improving TCP's Robustness to Blind In-Window Attacks*", IETF Internet Draft, keskeneräinen, viitattu versio: draft-ietf-tcpm-tcpsecure-07.txt, helmikuu 2007, 26 s.

[Rek96] Yakov Rekhter, Robert G Moskowitz, Daniel Karrenberg, Geert Jan de Groot & Eliot Lear, "*Address Allocation for Private Internets*", IETF RFC 1918, helmikuu 1996, 9 s.

[Rek01] Yakov Rekhter & Eric Rosen, "*Carrying Label Information in BGP-4*", IETF RFC 3107, toukokuu 2001, 8 s.

[Rek06] Yakov Rekhter, Tony Li & Susan Hares, "*A Border Gateway Protocol 4 (BGP-4)*", IETF RFC 4271, tammikuu 2006, 104 s.

[Rek07] Yakov Rekhter, Ronald P. Bonica & Eric C. Rosen, “*Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks*”, IETF RFC 4797, tammikuu 2007, 10s.

[Rie05] Maximilian Riegel, "*Requirements for Edge-to-Edge Emulation of Time Division Multiplexed (TDM) Circuits over Packet Switching Networks*", IETF RFC 4197, lokakuu 2005, 24 s.

[Ros01a] Eric C. Rosen, Arun Viswanathan & Ross Callon, "*Multiprotocol Label Switching Architecture*", IETF RFC 3031, tammikuu 2001, 61 s.

[Ros01b] Eric C. Rosen, Dan Tappan, Yakov Rekhter, Guy Fedorkow, Dino Farinacci, Tony Li & Alex Conta, "*MPLS Label Stack Encoding*", IETF RFC 3032, tammikuu 2001, 23 s.

[Ros06a] Eric C. Rosen & Yakov Rekhter, "*BGP/MPLS IP Virtual Private Networks (VPNs)*", IETF RFC 4364, helmikuu 2006, 47 s.

[Ros07] Carsten Rossenhövel, "*Test report. Multi-Vendor MPLS Interoperability Event*", EANTC/MFA Forum, Paris, helmikuu 2007, saatavissa: <http://www.mfaforum.org/tech/EANTC_MPLSWC07_WhitePaper_v12p.pdf>, viitattu: 29.4.2007.

[Ros05] Eric C. Rosen, Jeremy De Clercq, Olivier Paridaens, Yves T'Joens & Chandru Sargor, "*Use of PE-PE IPsec in RFC2547 VPNs*", IETF Internet Draft, keskeneräinen, viitattu versio: draft-ietf-l3vpn-ipsec-2547-05.txt, elokuu 2005, 18s.

[Ros06b] Eric Rosen, Wei Luo, Bruce Davie & Vasile Radoaca, "*Provisioning, Autodiscovery, and Signaling in L2VPNs*", IETF Internet Draft, keskeneräinen, viitattu versio: draft-ietf-l2vpn-signaling-08.txt, toukokuu 2006, 39 s.

[Sajassi] Ali Sajassi, "*VPLS Architectures*", seminaariesitelmä, IETF 53, maaliskuu 2002, 27s., saatavissa: <http://www.ietf.org/proceedings/02mar/slides/ppvpn-10.pdf>, viitattu: 22.5.2007.

[San06] Srihari R. Sangli & Daniel Tappan & Yakov Rekhter, "*BGP Extended Communities Attribute*", IETF RFC 4360, helmikuu 2006, 12 s.

[Sch07] Tom Scholl, ”*BGP MD5: Good, Bad, Ugly?*”, esitelmä, Nanog 39, helmikuu 2007, 19 s., esitys saatavissa: <http://www.nanog.org/mtg-0702/presentations/Scholl.pdf>, viitattu 17.5.2007.

[Sha06] Himanshu Shah, Eric Rosen, Francois Le Faucheur & Giles Heron, "*IP-Only LAN Service (IPLS)*", IETF Internet Draft, keskeneräinen, viitattu versio: draft-ietf-l2vpn-ipls-06.txt, kesäkuu 2006, 22 s.

[Smi06] Philip Smith & Christian Panigl, "*RIPE Routing Working Group Recommendations on Route-flap Damping*", Ripe-378, toukokuu 2006, saatavissa: <http://www.ripe.net/ripe/docs/ripe-378.html>, viitattu: 10.6.2007.

[Swa05] George Swallow, Ping Pan & Alia Atlas, "*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*", IETF RFC 4090, toukokuu 2005, 38 s.

[Vai06] Alexander Vainshtein (toim.) & Yaakov Stein (toim.), "*Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*", IETF RFC 4553, kesäkuu 2006, 27 s.

[Vil98] Curtis Villamizar, Ravi Chandra & Ramesh Govindan, "*BGP Route Flap Damping*", IETF RFC 2439, marraskuu 1998, 37 s.

[Väl02] Harri Välimäki, ”*Leimakytkentää hyödyntävien virtuaaliverkkojen vertailu*”, Diplomityö, Teknillinen korkeakoulu, toukokuu 2002, 97 s.

[Wan05] Xiaoyun Wang & Hongbo Yu, "*How to Break MD5 and Other Hash Functions*". EUROCRYPT 2005 -seminaarin esitelmä, ISBN 3-540-25910-4, 17 s., esitys saatavissa: <http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf>, viitattu: 17.5.2007.

[Whi03] Russ White, "*Securing BGP Through Secure Origin BGP*", The Internet Protocol Journal - Volume 6, Number 3, syyskuu 2003, s. 15-22. luettavissa: <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html>, viitattu 22.5.2007.

[Wik07] Wikipedia, ”*Multiprotocol Label Switching”*, luettavissa: <http://en.wikipedia.org/wiki/Multiprotocol_Label_Switching>, viitattu: 21.4.2007

[Wor05] Tom Worster, Yakov Rekhter & Eric Rosen, ”*Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*”, IETF RFC 4023, maaliskuu 2005, 14 s.

[Xia04] XiPeng Xiao (toim.), Danny McPherson (toim.), Prayson Pate (toim.), Vijay Gill, Kireeti Kompella, Thomas D. Nadeau & Craig White, “*Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*”, IETF RFC 3916, syyskuu 2004, 19 s.

liite A:
Tarkempi pohdinta vertailun tuloksista

Tutkimuksen vertailun tuloksia voi analysoida hieman tarkemmin tarkastelemalla, mihin osa-alueeseen kriteerin ”paljastama” ”tietoturva-aukko” vaikuttaa. Olen jakanut kriteerit kolmelle osa-alueelle sen mukaan, mihin niillä on ensisijainen vaikutus: operaattorin oma palvelualusta eli runkoverkko, inter-AS-VPN-palvelun asiakkaat ja intra-AS-VPN-asiakkaat. Tämä jaottelu on esitetty taulukossa A1. On huomattava, että runkoverkkoon kohdistuvat tietoturvauhat voivat välillisesti vaikuttaa sekä inter- että intra-AS-asiakkaisiin, kun taas tässä taulukossa inter ja intra-AS-VPN:ien alle laitetut kriteerit eivät vaikuta muihin osa-alueisiin.

Taulukko A1. Osa-alueet, joiden tietoturvaan kriteeri liittyy

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
runko-verkko				(x)		x	x	x							x		
Inter-AS-VPN	x	x	x	x	x			x	x	x		x	x	x	x	x	x
Intra-AS-VPN			(x)					x			x						

Taulukosta A1 käy selkeästi ilmi, että valtaosa kriteereistä liittyy ainoastaan inter-AS-asiakkaisiin; vain seitsemän kriteeriä vaikuttaa joko runkoverkkon tai intra-AS-VPN:ien tietoturvaan. Nämä seitsemän ”ydinkriteeriä” on poimittu seuraavan sivun taulukkoon A2. Tässä liitteessä syvennytään vielä hieman tähän taulukkoon ja sen tietojen käyttämiseen.

Taulukko A2. Vertailun ydinkriteerit

#	Kriteeri	A	B	C	D
3	Voidaanko vastaanotettavien VPN-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?				
4	Voidaanko vastaanotettavien IP-reittien määrää rajoittaa muuten kuin AS-kohtaisesti?				
6	Voidaanko PE- ja muiden reitittimien osoitteet jättää mainostamatta muihin AS:in?				
7	Voidaanko PE- ja muissa runkoverkon reitittimissä käyttää yksityisiä IP-osoitteita?				
8	Tarvitseeko runkoreitittimissä olla tunnelien päätepisteitä, joihin voi liikennöidä AS:n ulkopuolelta?				
11	Mahdollistaako arkkitehtuuri reittisuodatuksen inter-AS-RT:n tai vastaavan attribuutin perusteella?				
15	Onko rajareititin itse kaikkien leimojen myöntäjä, jotka toisesta verkosta tulevien pakettien leimapinoissa saa olla?				

Taulukosta A2 näkee selvästi, että eri yhteenliittämistavoilla on eroa[79] tietoturvan kannalta. Vertailun tulosten soveltamiseksi ne on suhteutettava tarpeisiin – lähinnä luottamuksen asteeseen kahden verkon välillä. Seuraavissa pohdin yhteenliittämismalli kerrallaan lyhyesti, mitä tulokset voisivat tarkoittaa käytännössä.

[79] Liikennevalovärityksen mukaisesti vihreä on hyvä ominaisuus ja punainen huono. Keltainen tarkoittaa määrittelemätöntä ja oranssi lievästi huonoa.

Mallin A tietoturva

Malli A on tämän tutkielman mukaan kaikkein tietoturvallisin. Se läpäisee kaikki kriteerit, jotka koskevat operaattoria ja intra-AS-asiakkaita. Sillä ei ole intra-AS-asiakkaisiin tai operaattorin omaan tietoturvaan liittyviä merkittäviä puutteita. Inter-AS-asiakkaiden osalta mallilla A oli kolme puutetta (kriteerit 10, 13 ja 16; taulukko 7 luvussa 5). Puutteet kriteerien 10 ja 13 kohdalla liittyvät kumppaniverkon sisäisen tietoturvan tasoon eli kumppanioperaattorin käytäntöjen tietoturvallisuuden tasoon. Tältä osin kyseessä on siis *luottamuksen määrä operaattoreiden välillä koskien yhteisten asiakkaiden yhteyksiä*. Jos asiakas tietää, minkä verkkojen kautta hänen yhteytensä kulkevat, ja asiakas luottaan kaikkien näiden verkkojen (operaattoreiden) tietoturvaan, mallin A tietoturva on riittävä. Jos asiakas ei luota kaikkien operaattoreiden tietoturvaan, on mahdollista käyttää salausta CE-reititinten välillä.

Kriteeri 16 liittyy kahteen asiaan. Ensinnäkin mallissa A konfiguroitavien laitteiden määrä kasvaa, mikä lisää aina riskiä virhekonfiguroinneille. Toiseksi se tarkoittaa, että mallissa A transit-operaattorin on osallistuttava VPN-signalointiin. Muissa malleissa VPN-signalointi voidaan ohjata transit-operaatorin ohi (esimerkiksi salausta käyttämällä), jolloin se ei ole altis transit-operaattorin virheille taikka salakuuntelulle.

Mallin B tietoturva

Malli B on taulukon A2 värejä laskemalla toiseksi tietoturvallisin kahdella punaisella merkinnällä, jotka koskevat operaattoria ja intra-AS-asiakkaita. Näistä kriteerin kolme – VPN-reittien määrän VPN-kohtainen rajoitus – ilmaisema puute on mahdollista kiertää kahdella eri tavalla: joko luottamalla siihen, että kumppanioperaattori huolehtii tästä rajoituksesta[80] tai sitten rajoittamalla VPN-reittien määrää kokonaisuutena. Jälkimmäinen tapa käytännössä sulkee kaikki AS-rajan yli menevät yhteydet, jos rajan ylittävien VPN-reittien määrä kasvaa liiaksi. Jompikumpi vaihtoehto on yleensä operaattorin hyväksyttävissä; kumpaa operaattori haluaa käyttää, riippuu luottamuksen määrästä operaattorien välillä.

Toinen kriteeri, jossa malli B pärjää huonosti, on kriteeri kahdeksan. Mallissa B tämä heikkous liittyy ASBR-reitittimen puuttuvaan kykyyn suodattaa liikennettä sisään tulevien pakettien leimojen perusteella. Näin ollen kaikki leimapolut, joihin ASBR voi lähettää liikennettä, ovat avoinna myös naapuri-AS:ään. Tämä haavoittuvuus liittyy leimakytkennän käytännön toteutukseen (ainakin Ciscon reitittimissä [Beh05]), eikä

[80] Asiakaskohtainen rajoitus on tehtävissä PE-reitittimessä.

välttämättä koske kaikkia reititinvalmistajia[81]. Tämä turvallisuusaukko on myös mahdollista tukkia käyttämällä kahta ASBR-reititintä peräkkäin [Beh05].

Inter-AS-asiakkaiden tietoturvaan liittyen mallissa B on mallin A puutteiden lisäksi kaksi puutetta enemmän (kriteerit 1, 14; taulukko 7). Yhteiset puutteet (10, 13) vaikuttavat mallissa B samoin kuin mallissa A.

Kriteeri yksi liittyy reittimainostusten tiheyteen. BGP:lle on mahdollista määritellä naapurin laitto jäähylle, jos reitit ovat liian epävakaat (häilyvien reittien vaimennus). BGP:n osalta naapurioperaattorin virhekonfiguraatio johtaisi siis kyseisen naapurin kautta menevän liikenteen pysähtymiseen. LDP:ssä ei ole vastaavaa mekanismia tällä hetkellä. Näin on olemassa teoreettinen mahdollisuus, että naapurioperaattorin vihrekonfiguraatio heiluttaisi operaattorin omaa hallintatasoa. Näin ollen *mallia B ei voi suositella, jos kumppanioperaattorin (ASBR:n) konfiguraatioiden virheettömyyteen ei luoteta ja lisäksi AS:ien välillä käytetään LDP-protokollaa* (käytännössä tämä tarkoittaa L2-VPN:iä, joita ei konfiguroida staattisesti).

Kriteeri 14 ei ole yhtä kriittinen, sillä asiakaskohtaisia liikenteenrajoituksia ei ylipäänsä tehdä yleensä runkoverkossa, jollaiseksi rajareititinten välinen yhteyskin voidaan laskea. Tämän rajoituksen puute voi kostautua muille inter-AS-VPN-asiakkaille, jos joko rajareititinten välisen linkin mitoitus ei ole oikea suhteessa inter-AS-asiakkaiden liikenneprofiileihin, tai kumppanioperaattori ei tee asiakkaan liikenteen rajoitusta silloin, kun liikenne tulee verkkoon[82]. Ensimmäinen näistä liittyy isompaan kokonaisuuteen: miten operaattorit saavat yhdistettyä palvelunlaatukonseptinsa. Toisessa taas palataan operaattoreiden keskinäiseen luottamukseen: luotetaanko, että toinen tekee sen, mitä lupaa. Toisaalta inter-AS-asiakkaat ovat joka tapauksessa operaattoreiden yhteisiä[83] ja liikennesuunnasta voi päätellä syyllisen. Tilanne on siis helpompi selvittää kuin tilanne, jossa pullonkaula on jossain muualla kuin AS-rajalla.

Mallin C tietoturva

Taulukon A2 valossa malli C on varsin tietoturvaton. Käyn tässä lyhyesti läpi kriteerit, joiden suhteen mallissa C oli puutteita. Kriteeri kolme: samat asiat pätevät kuin malliin B eli ongelma on kierrettävissä hyväksyttävästi. Kriteeri 4: IP-reittien liiallinen lukumäärä. Tämä ongelma riippuu siitä, halutaanko samalla ASBR:llä välittää sekä

---

[81] Muiden valmistajien osalta asiasta ei ole mainittu – niin kuin ei Ciscollakaan normaalimateriaalissa.

[82] Tämä tulisi tehdä joko PE- tai CE-reitittimessä.

[83] Vaikka eivät olisikaan suorassa sopimussuhteessa molempiin.

Internet- että VPN-liikennettä. Suositeltavaa olisi hoitaa VPN-peeraus erillisellä reitittimellä, jolloin hyväksyttävät reitit voi suodattaa: vain PE-reititinten, reittiheijastimien ja VPLS-keskittimien osoitteet hyväksytään. Jos käytetään samaa ASBR-reititintä sekä Internet- että VPN-liikenteelle, on VPN-palvelu mallissa C altis Internetin kautta tuleville reitityshäiriöille. Tätä riskiä on mahdollista pienentää lähinnä reitittimen käytössä olevaa muistia kasvattamalla.

Kriteeri kuusi PE-reititinten osoitteiden mainostamisesta naapuri-AS:ään nähdään joskus tietoturvakysymyksenä. Ensinnäkin kannattaa muistaa, että reitin mainostus ei ole sama asia kuin pääsyn takaaminen: mainostettuun osoitteeseen suuntautuva liikenne voidaan suodattaa ja toisaalta osoitteeseen, jota ei ole mainostettu, voidaan lähettää liikennettä esimerkiksi oletusreitityksen avulla. Tämän – ns. piilotetun runkoverkon – ohella toinen kysymys on operaattorin halukkuus paljastaa PE-reititintensä määrä toiselle operaattorille. Piilotetun runkoverkon käytön siunauksellisuudesta ei olla yhtä mieltä [Beh05], kun taas PE-reititinten määrän strategisen luonteen jokainen operaattori päättää itse. Kriteeri seitsemän – yksityisten IP-osoitteiden käytöstä – liittyy myös piilotetun runkoverkon käyttöön (lisäksi se on usein automaattisesti blokattu).

Mallissa C kriteerin 8 heikkous liittyy siihen, että PE-reitittimissä on kuljetustunnelin päät, jotka ovat saavutettavissa toisesta AS:stä. Nämä ovat olemassa VPN-liikenteen kuljettamista varten, mutta ASBR – tai mikään muukaan reititin matkalla – ei osaa päätellä yksittäisestä paketista, onko se VPN-liikennettä vai jotain muuta[84]. Näin ollen toisesta AS:stä tulevan, kuljetusleiman alla olevan paketin sisältö – otsakkeet mukaan lukien – voi olla mitä vain, esimerkiksi IP-otsake, jossa on jonkin normaalisti verkon ulkopuolelta pääsemättömissä olevan kohteen osoite. Vaihtoehtoisesti siellä voi olla VPN-leima, joka vie intra-AS-VPN:ään. Se, mitä PE-reititin, johon kuljetustunneli päättyy, tekee tunnelista tulevalle paketille, ei ole määritelty missään standardeissa, vaan riippuu sekä kyseisen PE-reitittimen ominaisuuksista että konfiguraatiosta. Tämän tyyppiset tietoturva-aukot voivat olla erittäin haastavia, sillä ne vaativat toimia muualla kuin itse verkkorajapinnassa. *Tämä on mallin C suurin tietoturvariski.* Kuvatun kaltainen liikenne voi alkaa vain kumppanioperaattorin leimakytketyltä alueelta. Tässäkin on kyse siis luottamuksen tasosta kumppanioperaattoriin ja sen tietoturvakäytöntöihin.

---

[84] Itse asiassa rajareititin on signaloinut vain IP-osoite+leima –parin, eikä signaloinnni avaulla muodostuvan leimapolun käytöstä ei mitään.

Kriteeri 15 liittyy mallissa C kriteeriin 8. Se korostaa, ettei ASBR tiedä paketin sisemmistä leimoista tai niiden puutteesta mitään, joten se ei voi tehdä suodatusta sisempien leimojen (tai niiden puutteen) perusteella, vaikka näin haluttaisiinkin.

Inter-AS-asiakkaiden tietoturvaan liittyen mallissa C on neljä puutetta, joita mallilla B ei ole (kriteerit 2, 5, 9, 16; taulukko 7) ja kolme yhteistä kriteeriä (1, 10 ja 14). Kriteerin yksi osalta malliin C pätevät samat asiat kuin malliin B: *mallia C ei voi suositella, jos kumppanioperaattorin (ASBR:n) konfiguraatioden virheettömyyteen ei luoteta ja lisäksi AS:ien välillä käytetään LDP-protokolla* (käytännössä tämä tarkoittaa L2-VPN:iä, joita ei konfiguroida staattisesti). Kriteerin kymmenen osalta malli C poikkeaa mallista B: siinä osa signaloinnista voi olla suoraan PE-reititinten välistä ja voi näin ollen varmentaa signaloinnin alkuperän paremmin. Kriteerin 14 osalta malli C vastaan mallia B: se ei ole varsinainen ongelma.

Kriteeri kaksi koskee IP-reittien välitykseen käytettävän BGP-protokollan viestien lähetystiheyttä. Liiallinen viestien tiheys johtuu väärin toimivasta naapurin rajareitittimestä ja se johtaa joko naapuruuden alasmenoon (jos BGP flap damping on käytössä) tai oman rajareitittimen kaatumiseen. Riippuen verkon topologiasta, tämä haittaa vain näiden verkkojen välistä inter-AS-liikennettä. Tämä on siis hyväksyttävä riski: tietyn operaattorin kanssa liikenne ei joissain tilanteissa toimi. Riski liittyy ennemmin kumppanioperaattorin valintaan kuin yhteenliittämistapaan.

Kriteeri viisi ilmaisee tietoturva-aukon, jossa väärä operaattori yrittää viedä toiselle operaattorille tarkoitettua liikennettä mainostamalla tämän PE-osoitetta. Tämä on mahdollista vain tietyissä verkkotopologioissa, sillä käytetty reitti valitaan lyhimmän AS-polun perusteella. Lisäksi tämä on estettävissä suodattamalla vastaanotettavia reittimainostuksia. Riippuen AS-topologiasta, ja siitä, halutaanko käyttää varmistusta samalle reitille eri AS:ien kautta, tämä turva-aukko voi olla mahdoton estää. Tällaisissa tilanteissa CE-reititinten välinen salaus on mahdollinen ratkaisu.

Mallin C kohtuullisen huono arvio kriteerin yhdeksän osalla johtuu potentiaalisesti suuresta määrästä signalointiyhteyksiä AS:ien välillä. Jos kaikki AS:ien väliset signalointiyhteydet halutaan varmistaa salasanoihin perustuvalla tekniikalla (esimerkiksi MD5:ttä käyttäen) eikä kaikkiin haluta käyttää samaa salasanaa, tulee salasanojen hallinnasta sitä vaikeampaa, mitä enemmän yhteyksiä on. Käytännössä muiden VPN-palveluiden kuin virtuaalijohtimien yhteyksiä pystytään keskittämään harvoille kokoaville signaloijille (reittiheijastin ja VPLS-hubi). Moniosaiset virtuaalijohtimet voivat kenties tuoda avun myös virtuaalijohtimien signaloinnin aggregointiin.

Kriteerillä 16 viitataan tilanteeseen, jossa toiselle operaattorille ei haluta antaa VPN-asiakkaan topologiasta yhtä tarkkaa kuvaa kuin mitä operaattorilla itsellään on. Koska

mallissa C kaikki inter-AS-VPN:iin liittyvä tieto välitetään toiselle operaattorille, välittyy sinne myös tieto VPN-asiakkaan topologiasta. Yleensä tätä ei varmasti nähdä ongelmana, mutta saattaa olla asiakkaita, joille se on.

Malli D:n tietoturva

Mallissa D ei Internet-liikennettä ja VPN-liikennettä voi mielekkäästi erottaa toisistaan, näin ollen siinä VPN-liikenne kärsii IP-reitityksen mahdollisista ongelmista – sekä tahallisista tai tahattomista (kriteerit 2 ja 4). VPN-liikennettä voi myös harhauttaa väärään paikkaan väärillä reittimainostuksilla (kriteeri 5). PE-reitittimillä tulee olla julkiset osoitteet, joita mainostetaan ainakin kumppanioperaattorille[85] (kriteerit 6 ja 7). PE-reitittimissä on AS:n ulkopuolelta tulevalle liikenteelle avoimia tunnelinpäitä (kriteeri 8), mutta näiden ei tarvitse olla kaikille avoimia, eikä kaikkien saavutettavissa[86]. Signalointikumppaneita mallissa tulee melko runsaasti (kriteeri 9), jos tavoitellaan laajaa palvelua. VPN-liikennettä ei käytännössä kohdella missään muusta IP-liikenteestä poikkeavasti, puhumattakaan virtuaaliverkkokohtaisesta palvelusta (kriteeri 14). Asiakkaan VPN-topologia paljastuu mallissa D samoin kuin mallissa C.

[85] Mallissa D kumppanioperaattorin käsite voi olla epämääräinen ja käytännössä Internet.

[86] Saavutettavuutta voidaan rajoittaa käyttämällä IPsec-tunnelointia ja liikenteen suodatusta.